

Endpoint Security Client

Benutzerhandbuch
R72



Check Point
SOFTWARE TECHNOLOGIES LTD.

© 2003-2009 Check Point Software Technologies

Alle Rechte vorbehalten. Dieses Produkt und die damit verbundene Dokumentation ist durch Urheberrechte geschützt und wird unter Lizenzierung vertrieben, die das Verwenden, Kopieren und Dekompilieren einschränkt. Ohne vorherige Zustimmung von Check Point darf kein Teil dieses Produkts oder der verbundenen Dokumentation in irgendeiner Form oder mit irgendwelchen Methoden reproduziert werden. Dieses Benutzerhandbuch wurde mit Sorgfalt erstellt, dennoch übernimmt Check Point keine Verantwortung für Fehler oder Auslassungen. Diese Publikation und die darin beschriebenen Funktionen können ohne Mitteilung geändert werden.

ERKLÄRUNG EINGESCHRÄNKTER RECHTE:

Die Verwendung, Vervielfältigung oder Offenlegung durch die Regierung unterliegt den Einschränkungen in Unterparagraph (c)(1)(ii) der Klausel Rights in Technical Data and Computer Software unter DFARS 252.227-7013 und FAR 52.227-19.

WARENZEICHEN:

Eine Liste unserer Marken finden Sie unter
<http://www.checkpoint.com/copyright.html>

Hinweise zu Dritten finden Sie unter:
http://www.checkpoint.com/3rd_party_copyright.html

Inhalt

Einführung in Endpoint Security	11
Führung durch das Endpoint Security-Hauptseite	11
Navigieren durch das Endpoint Security-Hauptseite	12
Taskleisten-Symbole	12
Bildschirme	13
Bildschirm „Überblick“	14
Reagieren auf Warnungen.....	18
Warnung „Neues Programm“	18
Warnung „Neues Netzwerk“ und VPN-Warnungen.....	19
Einhaltungswarnungen	19
VPN	21
VPN – Grundlagen	21
Typen von Endpoint Security VPNs.....	22
Kompakte und erweiterte VPN-Oberflächen.....	22
Starten und Beenden von VPN-Client-Diensten.....	23
Authentifizierung.....	24
Ändern von Authentifizierungsverfahren	24
Verwalten von Zertifikaten	25
Konfigurieren von Profilen und Sites	31
Verwalten von Verbindungsprofilen	32
Verwalten von VPN-Sites	36
Herstellen und Trennen von Verbindungen	41
Verbindungsstatus	42
Konfigurieren von Verbindungsoptionen	46
Erweiterte Konfigurationsoptionen	53
Deaktivieren von Popup-Meldungen.....	53
NAT Traversal Tunneling	53
Befehlszeilenoptionen.....	54

Antivirus und Anti-Spyware	57
Endpoint Security Antivirus und Anti-Spyware.....	57
Antivirus und Anti-Spyware aktivieren	57
Anzeigen des Viren- und Spyware-Schutzstatus	58
Aktualisieren von Antivirus und Anti-Spyware.....	58
Prüfen	59
Grundlegendes zu Prüfungsergebnissen.....	60
Manuelle Behandlung von Dateien	60
Senden von Viren und Spyware an Check Point	61
Anzeigen von Elementen in Quarantäne.....	62
Anzeigen von Protokollen	63
Erweiterte Optionen.....	65
Planen von Prüfungen	65
Aktualisieren von Viren- und Spyware-Definitionen	66
Festlegen von Zielen für die Prüfung	67
Prüfen bei Zugriff.....	68
Angaben von Spyware-Erkennungsmethoden.....	69
Aktivieren der automatischen Virenbehandlung	69
Aktivieren der automatischen Spyware-Behandlung	70
Reparieren von Dateien in einem Archiv	70
Optionen für die Virenprüfung	71
Antivirus-Ausnahmenliste	72
Anti-Spyware Ausnahmeliste	73
Firewall.....	75
Firewall-Schutz verstehen	75
Grundlegendes zu Zonen.....	76
Verwaltung der Firewall-Sicherheit nach Zonen	76
Program Control über Zonen.....	77
Konfigurieren neuer Netzwerkverbindungen	78
Integrieren in Netzwerkdienste	78
Aktivieren der Datei- und Druckerfreigabe.....	79

Herstellen einer Verbindung zu Netzwerk-Mailservern.....	79
Aktivieren der gemeinsamen Nutzung einer Internetverbindung ("Internet Connection Sharing", ICS)	80
Auswählen der Sicherheitsstufen.....	80
Festlegen von erweiterten Sicherheitsoptionen	81
Festlegen von Gateway-Sicherheitsoptionen	81
Festlegen von ICS-Optionen.....	82
Festlegen allgemeiner Sicherheitsoptionen.....	83
Festlegen von Netzwerk-Sicherheitsoptionen	85
Verwalten von Zonendatenverkehr	85
Anzeigen von Zonendatenverkehr	86
Ändern von Zonen-Datenverkehrsquellen.....	86
Hinzufügen zur Sicheren Zone	87
Hinzufügen zur Gesperrten Zone	89
Sperren und Freigeben von Ports	89
Einstellungen für Standard-Portberechtigungen	89
Hinzufügen benutzerdefinierter Ports	91
Konfigurieren der VPN-Verbindung für Firewall.....	92
Unterstützte VPN-Protokolle	92
Konfigurieren der VPN-Verbindung.....	93
Program Control	97
Grundlegendes zu Program Control.....	97
Zugriffssteuerung für Programme	97
Programmauthentifizierung	98
Festlegen der Optionen von Program Control	98
Festlegen der Sicherheitsstufe für Program Control	99
Aktivieren der automatischen Sperre	100
Konfigurieren des Programmzugriffs	101
Einstellen der Zugriffsrechte für Programme	101
Anpassen der Einstellungen von Program Control.....	102
Einstellen spezifischer Berechtigungen.....	103
Verwenden der Programmliste.....	103

Hinzufügen von Programmen zur Programmliste.....	104
Gewähren von Internet-Zugriffsrechten für Programme.....	105
Erteilen der Serverberechtigung für Programme.....	106
Erteilen der Berechtigung zum Senden von E-Mails für Programme.....	106
Erweiterte Einstellungen für Program Control	106
Deaktivieren des Schutzes für ausgehende E-Mails.....	107
Einstellen der Authentifizierungsoptionen.....	108
Zulassen der Verwendung von Programmen durch andere Benutzer	108
Verwalten von Programmkomponenten	108
Verwenden von Programmen mit dem Client	109
Verwenden von Antivirus-Software	109
Verwenden von Browsern	109
Verwenden von Chat-Programmen.....	110
Verwenden von E-Mail	110
Verwenden von internetbasierten Anrufbeantworterdiensten.....	111
Verwenden von Filesharing.....	111
Verwenden von FTP.....	111
Verwenden von Streaming Media	112
Verwenden von Spielen.....	112
Verwenden der Fernsteuerung	112
Verwenden von VNC	113
Verwenden von Voice over IP (VoIP)	113
Verwenden von Web Conferencing.....	114
Full Disk Encryption.....	115
Authentifizierung bei Full Disk Encryption	115
Ausschließen einer Computermanipulierung	116
Erstmalige Authentifizierung	116
Verwenden eines festen Kennworts	116
Verwenden eines dynamischen Tokens	118
Verwenden einer Smartcard/eines USB-Tokens	119
Vorgehensweise bei einem vergessenen Kennwort.....	121

Kein Zugriff auf den Token/die Smartcard	121
Optionale Full Disk Encryption-Funktionen.....	121
Synchronisieren von Kennwörtern.....	122
Single Sign-On und OneCheck Logon	123
Integrierte Windows-Anmeldung.....	125
Verwenden des Full Disk Encryption-Bildschirms	126
Anzeigen von Status- und Verschlüsselungsinformationen.....	126
Ändern der Anmeldeinformationen für die Authentifizierung	128
Ändern der Sprache für die Benutzeroberfläche	129
In der Vorstart-Umgebung unterstützte Zeichen	134
Media Encryption	135
Funktionen	135
Encryption Richtlinie Manager.....	136
Manager für Wechselmedien.....	136
Gerätemanager.....	137
Program Security Guard	137
Zwischengespeicherte Kennwörter.....	138
Verwenden des EPM Clients	139
Verschlüsseln von Medien	139
Verschlüsseln von CDs und DVDs	142
Zugreifen auf verschlüsselte Medien.....	142
Zugreifen auf verschlüsselte Medien von Computern ohne Media Encryption	144
Löschen von CDs oder DVDs	146
Ändern des Kennworts für das verschlüsselte Gerät.....	146
Verwenden des Managers für Wechselmedien	146
Autorisieren von Wechselmedien.....	146
Verwenden des Gerätemanagers	147
Verwenden von Program Security Guard	148
Bereich "Wartung"	148
WebCheck	149
Grundlegendes zu WebCheck.....	149

Schutz durch WebCheck	149
Internet-Modus und Unternehmensmodus	150
Warnungen vor verdächtigen Sites	151
Gelber Meldebanner	151
Rote Warnung "Könnte Phishing sein"	152
Rote Warnmeldungen	153
E-Mail-Schutz.....	155
Schutz für ausgehenden MailSafeverkehr	155
Schutz für ausgehenden MailSafeverkehr	156
Anpassen des MailSafe-Schutzes für ausgehenden Datenverkehr	156
MailSafe nach Programm aktivieren	156
Schutz für ausgehenden MailSafeverkehr	157
Richtlinien	159
Richtlinie Typen	159
Grundlegendes zur Vermittlung zwischen Richtlinie	160
Anzeigen der verfügbaren Richtlinien	160
Verwenden des Bildschirms Richtlinien	160
Warnungen und Protokolle	163
Grundlegendes zu Warnungen und Protokollen	163
Informationen zu Warnungen.....	163
Informationen zur Ereignisprotokollierung.....	164
Einstellen grundlegender Warn- und Protokolloptionen.....	165
Festlegen der Warnungsereignisstufe	165
Festlegen der Ereignis- und Programmprotokollierungsoptionen	165
Ein- und Ausblenden von Warnungen	166
Ein- und Ausblenden von Firewall-Warnungen.....	166
Festlegen der Ereignis- und Programmprotokollierungsoptionen	167
Format der Protokollarchivierung	167
Anpassen der Ereignisprotokollierung.....	167
Anpassen der Programmprotokollierung.....	168
Anzeigen von Protokolleinträgen	168

Anzeigen des Textprotokolls.....	170
Archivieren von Protokolleinträgen	171
Verwenden von SmartDefense Advisor	172
Warnungsmeldungen - Referenz.....	173
Hinweise	173
Firewallmeldung/Geschützt.....	173
MailSafemeldung	175
Warnungen bei gesperrtem Programm	175
Meldungen für Internetsperre	176
Einhaltungswarnungen.....	177
Programmwarnungen	178
Warnung „Neues Programm“	178
Warnung „Bekanntes Programm“	179
Warnung „Geändertes Programm“	180
Warnung „Programmkomponente“	181
Warnung „Serverprogramm“	183
Erweiterte Programmwarnungen.....	185
Warnung „Manuelle Maßnahme erforderlich“	186
Warnung Neues Netzwerk.....	187
Fehlerbehebung	189
Fehlerbehebung bei VPN.....	189
Konfigurieren des Clients für VPN-Datenverkehr	190
Automatische VPN-Konfiguration und erweiterte Regeln.....	190
Automatische VPN-Erkennungsverzögerung.....	190
Fehlerbehebung für Netzwerke.....	191
Sichtbarmachen des Computers im lokalen Netzwerk.....	191
Lokales Freigeben von Dateien und Druckern	192
Beheben eines langsamen Systemstarts.....	192
Fehlerbehebung für die Internetverbindung.....	193
Fehlschlagen der Internetverbindung nach der Installation	193
Zulassen von ISP-Heartbeat-Signalen	194

Herstellen einer Verbindung über einen ICS-Client	195
Herstellen einer Verbindung über einen Proxyserver.....	196
Glossar	197
Index	211

Einführung in Endpoint Security

Check Point Endpoint Security™ ist der erste und einzige Agent, der alle wichtigen Komponenten für einen umfassenden Schutz des Endpunkt in sich vereint: erstklassige Firewall-, Antivirus-, Anti-Spyware-Software, Full Disk Encryption, Media Encryption mit Port-Schutz, Network Access Control (NAC), Program Control und VPN.

Mit Check Point Endpoint Security können Sie PCs schützen, ohne mehrere Agenten bereitstellen und verwalten zu müssen, was gleichzeitig Ihre Betriebskosten senkt.

Inhalt dieses Abschnitts

[Führung durch das Endpoint Security-Hauptseite](#)

11

[Reagieren auf Warnungen](#)

18

Führung durch das Endpoint Security-Hauptseite

Das Endpoint Security-Hauptseite ermöglicht den direkten Zugriff auf alle Sicherheitsfunktionen, die Ihren Computer schützen.

Sie starten das Endpoint Security-Hauptseite, indem Sie **Einstellungen** aus dem Taskleistenmenü von Endpoint Security auswählen.

Navigieren durch das Endpoint Security-Hauptseite

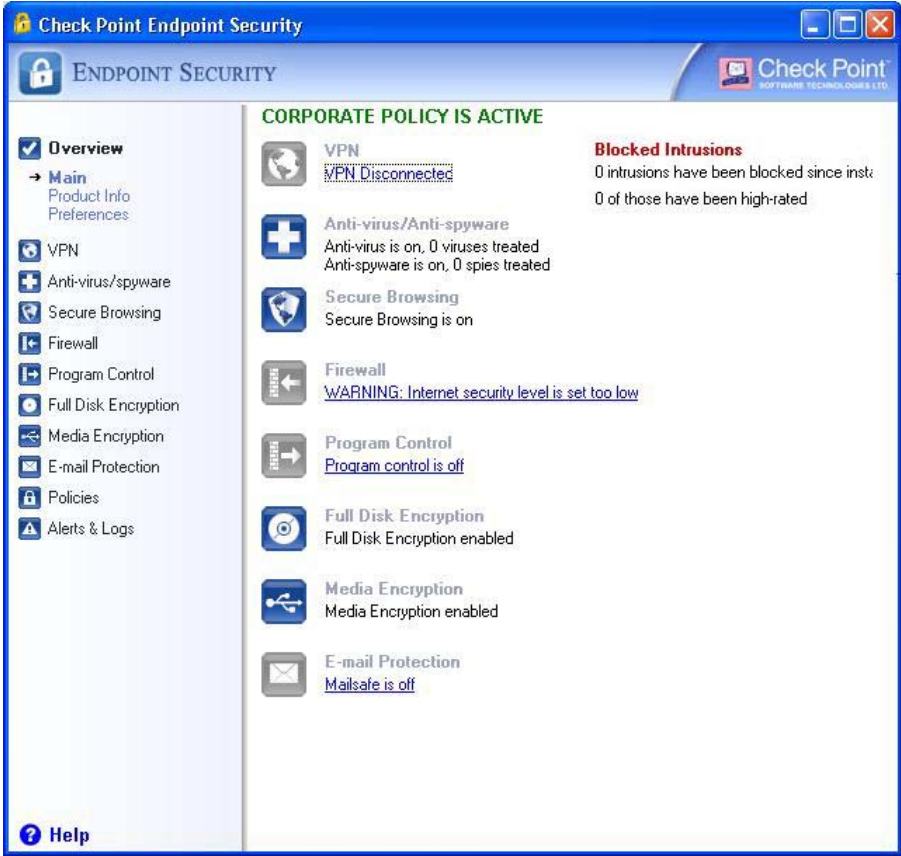


Figure - 1 Endpoint Security-Hauptseite

Über das Menü links haben Sie Zugriff auf die verfügbaren Bildschirme.

Taskleisten-Symbole

Über die Symbole in der Taskleiste können Sie Ihren Sicherheitsstatus und Ihre Internetaktivitäten jederzeit kontrollieren und haben mit nur wenigen Mausklicks Zugriff auf die Sicherheitseinstellungen. Klicken Sie mit der rechten Maustaste auf eines der folgenden Symbole, um ein Kontextmenü zu öffnen.

Table 0- 1 Taskleisten-Symbole

Symbol	Beschreibung
	Verbindung mit VPN ist hergestellt.
	Eine Sicherheitsprüfung, Verschlüsselung oder Änderung an Client-Einstellungen wird gerade durchgeführt.
	Ihre Aufmerksamkeit ist gefordert. (Beispiel: Der Client hält Richtlinie nicht ein, ein Anwendungsfehler ist aufgetreten oder ein Neustart ist erforderlich).

Bildschirme

Für Ihren Endpoint Security Client stehen abhängig von der Installation und Konfiguration, die Ihr Administrator für Sie eingerichtet hat, einige oder alle Bildschirme zur Verfügung.

VPN

Zeigt an, ob Sie mit dem VPN verbunden sind, wenn Sie VPN auf Ihrem Endpoint Security Client installiert haben.

Antivirus / Anti-Spyware

Zeigt an, ob der jeweilige Schutz aktiviert ist und wie viele Viren und Spyware-Programme im Falle einer Aktivierung behandelt wurden.

Firewall

Gibt an, ob Ihre Firewall aktiv ist, und zeigt die Anzahl der Firewall und Internetsperre-Warnungen seit dem letzten Zurücksetzen an. Wenn eine Warnung angezeigt wird, klicken Sie auf den unterstrichenen Warnungstext, um direkt zu dem Bildschirm zu gelangen, auf dem Sie Ihre Einstellungen anpassen können.

Program Control

Gibt an, ob Program Control sicher konfiguriert ist, und zeigt die Anzahl der Programmwarnungen an, die seit dem letzten Zurücksetzen aufgetreten sind. Sie

werden von Endpoint Security Client gewarnt, wenn Program Control deaktiviert ist.

Full Disk Encryption

Bietet Zugang zu Optionen für Full Disk Encryption.

Media Encryption

Bietet Zugang zu Optionen für Media Encryption und den EPM Client.

WebCheck

Gibt an, welche WebCheck-Optionen für diesen Client vom Endpoint Security-Administrator bereitgestellt wurden.

E-Mail-Schutz

Gibt an, ob die MailSafe-Funktion aktiviert ist, und zeigt die Anzahl der Anhänge an, die seit dem letzten Zurücksetzen unter Quarantäne gestellt wurden. Klicken Sie bei Anzeige einer Warnung auf den unterstrichenen Warnungstext. Sie gelangen dann direkt zu dem Bildschirm, in dem Sie Ihre Einstellungen anpassen können.

Richtlinien

Zeigt eine Tabelle der verfügbaren Richtlinien sowie Informationen zur aktuell aktiven Richtlinie.

Bildschirm „Überblick“

Im Bildschirm Überblick können Sie die dringlichsten Angelegenheiten sofort angehen und den Status der verschiedenen Schutz- und Verbindungsbereiche schnell kontrollieren.

So öffnen Sie den Bildschirm „Überblick“:

1. Klicken Sie mit der rechten Maustaste auf das Taskleisten-Symbol von Endpoint Security.
2. Wählen Sie Einstellungen aus.

Im daraufhin geöffneten Endpoint Security Endpoint Security-Hauptseite wird der Bildschirm Überblick mit der Registerkarte, Grundeinstellungen angezeigt.

Verwenden der Registerkarte „Grundeinstellungen“ von „Überblick“

In der Registerkarte Grundeinstellungen des Bildschirms Überblick sehen Sie auf einen Blick, ob Ihre Firewall, Programm- und E-Mail-Sicherheitseinstellungen aktiviert sind. Außerdem wird eine Zusammenfassung der Sicherheitsaktivität angezeigt. Auf der Registerkarte Grundeinstellungen können Sie Folgendes tun:

- Auf einen Blick feststellen, ob Ihr Computer abgesichert ist
- Eine Zusammenfassung der Client-Aktivitäten anzeigen
- Überprüfen, ob Ihre Client-Version auf dem neuesten Stand ist
- Das Lernprogramm aufrufen

Festlegen von Voreinstellungen

Über die Registerkarte Überblick | Voreinstellungen haben Sie Zugriff auf allgemeine Einstellungen.

Festlegen des Kennworts auf Benutzerebene

Durch das Festlegen eines Kennworts auf Benutzerebene hindern Sie andere daran, Endpoint Security Client zu beenden, zu deinstallieren oder Ihre Sicherheitseinstellungen zu ändern. Durch Festlegen eines Kennworts werden andere Personen nicht am Zugriff auf das Internet von Ihrem Computer aus gehindert.

Falls Ihre Version von Endpoint Security Client von einem Administrator mit Installationskennwort installiert wurde, kann dieser Administrator auf alle Funktionen zugreifen.

Wenn Sie erstmals ein Kennwort festlegen, müssen Sie sich abmelden, ehe Sie den Computer verlassen, da ansonsten andere Benutzer Ihre Einstellungen ändern können.

Mit dieser Einstellung können andere Benutzer Programme verwenden und auf das Internet zugreifen, allerdings nicht Ihre Sicherheitseinstellungen ändern. Vielleicht möchten Sie beispielsweise verhindern, dass Ihre Kinder die Endpoint Security-Einstellungen ändern, ihnen jedoch trotzdem die Verwendung neuer Programme erlauben, ohne dass sie Ihr Kennwort kennen.



Hinweis - Programme, die sich bereits auf Ihrer Liste der gesperrten Programme befinden, können von anderen Benutzern nicht verwendet werden.

So legen Sie ein Kennwort für Endpoint Security Client fest oder ändern dieses:

1. Öffnen Sie Überblick|Voreinstellungen.
2. Klicken Sie auf Kennwort festlegen.
3. Geben Sie Ihr Kennwort und die Bestätigung des Kennworts in die angezeigten Felder ein.
4. Wählen Sie Anderen Benutzern die Verwendung von Programmen ohne Kennwort gestatten aus.
5. Klicken Sie auf OK.



Hinweis - Gültige Kennwörter müssen mindestens 6 und dürfen höchstens 31 Zeichen enthalten. Gültige Zeichen sind A bis Z, a bis z, 0 bis 9 sowie die Zeichen !, @, #, \$, %, ^, &, *.

Wenn Sie ein Kennwort festgelegt haben, müssen Sie sich anmelden, bevor Sie Einstellungen ändern, die TrueVector-Sicherheitsengine beenden oder Endpoint Security deinstallieren können.

Festlegen von allgemeinen Voreinstellungen

Standardmäßig startet der Client automatisch beim Hochfahren Ihres Computers. Über die Einstellungen im Bereich **Allgemein** können Sie die Option für den automatischen Start ändern.

So legen Sie allgemeine Voreinstellungen für die Anzeige fest:

1. Öffnen Sie Überblick| Voreinstellungen.
2. Wählen Sie im Bereich **Allgemein** Ihre Voreinstellungen aus.
 - **Beim Starten Check Point Endpoint Security Software laden:** Endpoint Security wird beim Hochfahren des Computers automatisch gestartet.
 - **Den Check Point Endpoint Security Client schützen:** Hindert Trojaner daran, Tastatur- und Mausabfragen an den Client zu schicken.

Um maximale Sicherheit zu gewährleisten, deaktivieren Sie diese Funktion nur, wenn Sie beim Verwenden von Remote-Programmen Probleme mit Ihrer Tastatur oder Maus haben.

Wenn Sie über diesen Computer eine Verbindung zu einem Proxyserver herstellen, klicken Sie auf **Optionen**. Geben Sie im Fenster **Optionen** die Proxyserver-Details an.

So konfigurieren Sie einen Proxyserver:

1. Wählen Sie Proxyserver aktivieren.

2. Geben Sie im Feld **Proxyserver** den Hostnamen oder die IP-Adresse des Proxyservers ein.
3. Geben Sie im Feld **Port** den offenen Port zwischen diesem Computer und dem Proxyserver an.
4. Klicken Sie auf **OK**.

Festlegen von Verbindungsvoreinstellungen

Durch Festlegen der Verbindungsvoreinstellungen wird sichergestellt, dass Ihre Privatsphäre geschützt ist, wenn der Client mit Check Point Daten austauscht (z. B. um automatisch nach Aktualisierungen zu suchen).

So legen Sie Verbindungsvoreinstellungen fest:

1. Öffnen Sie **Überblick|Voreinstellungen**.
 2. Wählen Sie im Verbindungsbereich Ihre Voreinstellungen aus.
 - **Vor Herstellung der Verbindung Popup-Fenster anzeigen:** Zeigt eine Warnung an, bevor Sie die Verbindung zu Check Point aufnehmen, um Registrierungsinformationen zu senden, Produktaktualisierungen herunterzuladen, weitere Informationen über eine Warnung zu suchen, oder auf DNS zuzugreifen, um IP-Adressen zu suchen.
-
- Hinweis - Wenn Sie sich an der Check Point Secure Community beteiligen, erhalten Sie vor dem Senden anonymer Daten keine Warnung.
- **IP-Adresse wenn möglich ausblenden:** Verhindert, dass Ihr Computer identifiziert werden kann, wenn Sie eine Verbindung zu Check Point herstellen.
 - **Letztes Oktett der IP-Adresse wenn möglich ausblenden:** Verhindert die Anzeige des letzten Teils Ihrer IP-Adresse (z. B. 123.456.789.XXX), wenn Sie eine Verbindung zu Check Point herstellen.

Grundlegendes zur Registerkarte "Produktinformationen"

Die Registerkarte **Überblick | Produktinformationen** enthält Versionsinformationen zu folgenden Komponenten:

- Endpoint Security Client (einschließlich Datum und Uhrzeit der Installation)
- TrueVector-Sicherheitsengine
- Treiber

- VPN-Engine (wenn zutreffend)
- Antivirus Engine
- Anti-Spyware Engine

Reagieren auf Warnungen

Wenn Sie den Client zum ersten Mal einsetzen, ist es normal, dass eine Vielzahl von Warnungen angezeigt wird. Der Endpoint Security Client macht sich lediglich mit Ihren Programm- und Netzwerkkonfigurationen vertraut und gibt Ihnen die Gelegenheit, die Sicherheit Ihren Anforderungen entsprechend einzustellen.

Wie Sie auf eine Warnung reagieren, hängt von der Art der angezeigten Warnung ab.

Warnung „Neues Programm“

Am Anfang wird vor allem die Warnung **Neues Programm** häufig angezeigt. Diese Warnung wird angezeigt, wenn ein Programm auf Ihrem Computer Zugriffsrechte oder Serverberechtigungen für das Internet oder Ihr lokales Netzwerk anfordert. Mit der Warnung **Neues Programm** können Sie den einzelnen Programmen die erforderlichen Zugriffsrechte erteilen (z. B. Ihrem Browser und E-Mail-Programm).



Hinweis - Aktivieren Sie das Kontrollkästchen **Diese Einstellung beim nächsten Start des Programms verwenden**, um vertrauenswürdigen Programmen permanente Zugriffsrechte zu gewähren.

Nur wenige Programme oder Prozesse benötigen eine Serverberechtigung, um ordnungsgemäß funktionieren zu können. Einige Prozesse werden jedoch von Microsoft Windows für die Ausführung vertrauenswürdiger Funktionen verwendet. Folgende Prozesse kommen häufig in Warnmeldungen vor:

- lsass.exe
- spoolsv.exe
- svchost.exe
- services.exe
- winlogon.exe

Sollten Sie das Programm oder den Vorgang, der eine Serverberechtigung anfordert, nicht erkennen, suchen Sie auf der Microsoft-Support-Website (<http://support.microsoft.com/>) nach Informationen, um festzustellen, um welchen Prozess es sich handelt und wozu er verwendet wird. Beachten Sie, dass viele vertrauenswürdige Windows-Prozesse (einschließlich der oben aufgeführten), von

Hackern verwendet werden können, um Würmer und Viren zu verbergen oder Trojanern Zugriff auf Ihr System zu ermöglichen. Wenn Sie bei der Anzeige einer Warnmeldung gerade keinen Vorgang durchgeführt haben (z.B. Durchsuchen von Dateien, Anmelden am Netzwerk oder Herunterladen von Dateien), dann ist es am sichersten, wenn Sie die Serverberechtigung verweigern. Sie können bestimmten Programmen und Diensten in der Programmliste jederzeit Zugriffsrechte gewähren, indem Sie die Registerkarte **Program Control | Programme** auswählen.

Werden viele Serverprogramm-Warnungen angezeigt, sollten Sie vorsichtshalber das Anti-Spyware-Programm ausführen.

Warnung „Neues Netzwerk“ und VPN-Warnungen

Am Anfang des Einsatzes des Sicherheitsprogramms werden wahrscheinlich auch Warnungen vom Typ "Neues Netzwerk" sowie VPN-Konfigurationswarnungen angezeigt. Diese Warnungen werden angezeigt, wenn der Client eine Netzwerk- oder VPN-Verbindung feststellt. Mit diesen Warnungen können Sie Ihre Sichere Zone, Port-/Protokollberechtigungen und Programmberechtigungen korrekt konfigurieren, so dass Sie über Ihr Netzwerk sicher arbeiten können.

Einhaltungswarnungen

Einhaltungswarnungen treten auf, wenn Endpoint Security Server in Verbindung mit Endpoint Security Client feststellt, dass Ihr Computer die Sicherheitsanforderungen des Unternehmens nicht erfüllt. Je nach Art der Nichterfüllung ist Ihr Zugriff auf das Unternehmensnetzwerk eventuell *eingeschränkt* oder sogar *unmöglich*.

Computer, auf denen die korrekten Typen und Versionen der erforderlichen Software ausgeführt werden, entsprechen i.d.R. den Sicherheitsanforderungen des Unternehmens. Wenn Endpoint Security allerdings feststellt, dass ein Computer diesen Anforderungen nicht entspricht, geschieht Folgendes:

- Es wird eine Einhaltungswarnung angezeigt (jedoch nur, wenn die Anzeige von Einhaltungswarnungen in der derzeit aktiven SicherheitsRichtlinie des Unternehmens aktiviert ist)
- Sie werden auf eine Webseite geleitet, auf der Sie erfahren, wie Sie Ihren Endpunkt Computer an die Anforderungen anpassen können.

Was weiterhin geschieht, hängt von den SicherheitsRichtlinien Ihres Unternehmens ab.

- Wenn das Problem nicht sofort behoben werden muss, ist Ihr Zugriff auf das Unternehmensnetzwerk möglicherweise *eingeschränkt*. Sie können weiterhin auf einige Ressourcen im Unternehmensnetzwerk zugreifen, bevor Sie die notwendigen Schritte durchführen, um Ihren Computer an die Anforderungen anzupassen.
- Wenn das Problem sofort behoben werden muss, ist der Zugriff auf das Unternehmensnetzwerk eventuell *unmöglich*. In diesem Fall können Sie nur auf die Webseite zugreifen, die Anweisungen dazu enthält, wie Sie Ihren Computer an die Sicherheitsanforderungen des Unternehmens anpassen können.

VPN

Bei einem Virtual Private Network (VPN) können Sie über das Internet per Fernzugriff eine Verbindung zum privaten Netzwerk oder Intranet Ihres Unternehmens herstellen. VPNs ermöglichen eine private und sichere Kommunikation, bei der die Daten über öffentliche Netzwerke wie das Internet übertragen werden.

Inhalt dieses Abschnitts

VPN – Grundlagen	21
Authentifizierung	24
Konfigurieren von Profilen und Sites	31
Herstellen und Trennen von Verbindungen	41
Erweiterte Konfigurationsoptionen	53

VPN – Grundlagen

Über Endpoint Security VPN können Sie per Fernzugriff eine sichere Verbindung zu Ihrem Unternehmensnetzwerk herstellen, wenn Sie nicht vor Ort arbeiten. Nachdem Ihr Computer und die VPN-Site sich gegenseitig einen Identitätsnachweis erbracht haben (oder sich *authentifiziert* haben), findet die gesamte nachfolgende Kommunikation in verschlüsselter und sicherer Form statt. Sie können dann über das Internet auf private Dateien zugreifen und wissen, dass unberechtigte Personen diese nicht anzeigen oder verändern können. Die VPN-Verbindung kann entweder direkt mit dem Server oder über einen Internetdienstanbieter (Internet Service Provider, ISP) hergestellt werden. Remote-Benutzer können die Verbindung zum Unternehmen mithilfe eines beliebigen Netzwerkadapters (einschließlich Wireless-Adapter) aufbauen oder sich per Modem einwählen.

Die VPN-Funktion von Endpoint Security authentifiziert die Kommunikationsteilnehmer und verschlüsselt die Daten, die zwischen ihnen übermittelt werden. Die starke Verschlüsselung und die Authentifizierung durch die VPN-Funktion erfolgen über standardmäßige Internetprotokolle. Durch die Verschlüsselung wird sicher gestellt, dass nur die authentifizierten Parteien die Daten lesen können, die zwischen ihnen übertragen werden. Darüber hinaus wird die Integrität der Daten gewährleistet, d.h., die Daten können während der Übertragung nicht verändert werden.

Im **VPN-Hauptfenster** werden Informationen zu allen derzeitigen VPN-Verbindungen (sofern vorhanden) und zum Status der Remote-Verbindung mit dem Endpoint Security-Server angezeigt. Über das **Hauptfenster** können Sie den Site-Assistenten starten, um eine VPN-Site zu erstellen, um eine Verbindung zu einer VPN-Site herzustellen oder diese zu trennen oder um das Fenster VPN-Einstellungen zu öffnen, in dem Sie Profile und Sites konfigurieren, alle spezifischen Verbindungsoptionen festlegen oder Zertifikate verwalten können.

Typen von Endpoint Security VPNs

Ihr Administrator hat für Ihren Client einen VPN-Typ konfiguriert. Dies ist entweder Check Point Endpoint Connect oder das alte Endpoint Security VPN. Die Ihnen zur Verfügung stehenden Optionen hängen davon ab, welches VPN für Ihren Client konfiguriert wurde.

Normalerweise stehen Ihnen die Check Point Endpoint Connect-Optionen zur Verfügung, wenn im Bildschirm **VPN | Grundeinstellungen** die VPN-Optionen angezeigt werden. Werden VPN-Einstellungen angezeigt, verfügen Sie über den alten Endpoint Security VPN-Client.

Kompakte und erweiterte VPN-Oberflächen

Wenn Ihr Endpoint Security Client mit einer Rechts-VPN konfiguriert ist, wird er entweder mit einer kompakten oder mit einer erweiterten Version der VPN-Oberfläche bereitgestellt.

Sie können die Versionen selbst ändern, wenn der Client ausgeführt wird.

In der Kompaktansicht wird die VPN-Oberfläche Benutzern, die nicht mehrere Sites oder Profile benötigen, in vereinfachter Form angezeigt.

Die erweiterte Ansicht eignet sich eher für erfahrene Benutzer, die eine Verbindung zu verschiedenen VPN-Sites herstellen müssen und ihre VPN-Konfiguration genauer verwalten möchten.

So wechseln Sie zwischen der erweiterten und der Kompaktansicht:

1. Wenn Sie von der erweiterten Ansicht zur Kompaktansicht wechseln, müssen Sie zunächst folgende Schritte ausführen:
 - a. Löschen Sie alle Sites (siehe **Löschen von Sites** auf Seite 40).
 - b. Deaktivieren Sie Auto Local Logon (siehe **Auto Local Logon** siehe "Auto Local Logon (Autom. lokale Anmeldung)" auf Seite 47 Autom. lokale Anmeldung).
 - c. Deaktivieren Sie Secure Domain Logon (Sichere Anmeldung über Domäne) (siehe **Secure Domain Logon** siehe "Secure Domain Logon (Sichere Anmeldung über Domäne)" auf Seite 47).
2. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.
3. Öffnen Sie die Registerkarte Erweiterte Einstellungen.
4. Wählen Sie im Bereich Product View (Produktansicht) die Option Extended View (Erweiterte Ansicht) oder Compact View (Kompaktansicht) aus, und klicken Sie auf OK.
5. Klicken Sie auf OK, um den Neustart von VPN-Diensten zu bestätigen.

Im Fenster VPN wird die Meldung angezeigt, dass die VPN-Dienste neu gestartet werden. Beim Wiederherstellen des Fensters VPN wird die ausgewählte Ansicht aktiviert.

Starten und Beenden von VPN-Client-Diensten

Wenn Ihr Endpoint Security Client für die Verwendung des Check Point Endpoint Connect VPN konfiguriert wurde, können Sie die VPN-Client-Dienste starten und beenden.

So starten Sie Endpoint Connect:

1. Start > Programme > Check Point Endpunkt VPN
2. Klicken Sie auf Check Point Endpunkt VPN.

So beenden Sie Endpoint Connect:

1. Klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste.
2. Wählen Sie die Option zum Beenden des Clients.

Authentifizierung

Wenn Sie eine Verbindung zu einer Site herstellen und dabei Identifikationsinformationen angeben, stellen Sie Authentifizierungsdaten bereit. Es sind zahlreiche Authentifizierungsverfahren verfügbar.

Wenden Sie sich an Ihren SystemAdministrator, damit er Ihnen eines der folgenden Elemente sendet:

- Registriertes Zertifikat (auf Diskette oder in Form eines Hardware-Tokens) und Kennwort (zum Öffnen des Zertifikats)
- Registrierungscode, mit dem Sie den Vorgang der Zertifikaterstellung online durchführen können
- Benutzername und Kennwort
- SecurID-Karte
- Antwortcode für eine Smartcard

Ändern von Authentifizierungsverfahren

Möglicherweise werden Sie von Ihrem Administrator zu einer Änderung des VPN-Authentifizierungsverfahrens aufgefordert. In diesem Fall sollte er Ihnen die Authentifizierungsdaten bereitstellen. Falls Ihr Laptop als Terminal für andere Benutzer fungiert (wobei jeder Benutzer, der eine Verbindung zur Site herstellt, über ein eigenes eindeutiges Zertifikat verfügt), müssen Sie gegebenenfalls das Zertifikat wechseln.



Hinweis - Beachten Sie, dass Sie Authentifizierungsverfahren bei bestehender Verbindung zu einer VPN-Site nicht ändern können.

Die Vorgehensweise zum Ändern von Authentifizierungsverfahren ist je nach Art des für Ihren Client konfigurierten VPNs unterschiedlich. Wählen Sie die für Ihren Client relevanten Anweisungen entsprechend den für Sie verfügbaren Optionen aus.

So ändern Sie Authentifizierungsverfahren:

1. Öffnen Sie VPN | Grundeinstellungen.
2. Wenn Sie mit einer VPN-Site verbunden sind, klicken Sie auf **Trennen**.
3. Wenn Sie die Schaltfläche **VPN-Einstellungen** sehen:
 - a. Klicken Sie auf **VPN-Einstellungen**.

- b. Wählen Sie auf der Registerkarte **Verbindungen** eine Site aus und klicken Sie auf **Eigenschaften**.
 - c. Öffnen Sie die Registerkarte **Authentifizierung**.
4. Wenn Sie die Schaltfläche **VPN-Optionen** sehen:
 - a. Klicken Sie auf **VPN-Optionen**.
 - b. Wählen Sie auf der Registerkarte **Sites** die relevante Site aus und klicken Sie auf **Eigenschaften**.
 - c. Öffnen Sie die Registerkarte **Einstellungen**.
5. Wählen Sie in der Dropdown-Liste **Scheme** (Schema) ein Authentifizierungsverfahren aus.
6. Geben Sie die entsprechenden Informationen für das Authentifizierungsverfahren ein.

Wenn Sie beispielsweise ein Zertifikat verwenden, klicken Sie auf **Durchsuchen**, und wählen Sie das Zertifikat aus.
7. Klicken Sie auf **OK**.

Wenn Sie erstmals ein VPN konfigurieren, wird im Fenster **First Time Configuration - Authentication Method** (Erstkonfiguration - Authentifizierungsverfahren) ebenfalls die Konfigurationsoption **Scheme** (Schema) angezeigt. Wählen Sie in der Dropdown-Liste **Scheme** (Schema) das Authentifizierungsverfahren aus, und klicken Sie dann auf **OK**.

Verwalten von Zertifikaten

Es empfiehlt sich, beim Aufbau einer VPN-Verbindung für die Authentifizierung digitale Zertifikate zu verwenden. Zertifikate sind sicherer als andere Verfahren wie eine Kombination aus Benutzername und Kennwort. Bei einer Authentifizierung mit Zertifikaten bestätigen der Client und die VPN-Site, dass das Zertifikat der jeweils anderen Seite von einer bekannten und vertrauenswürdigen Zertifizierungsstelle signiert wurde und dass es nicht abgelaufen ist oder widerrufen wurde.

Sie oder Ihr Administrator müssen sich bei einer Zertifizierungsstelle registrieren. Dies ist bei jeder beliebigen PKI-Zertifizierungsstelle (Public Key Infrastructure) eines Drittanbieters möglich, die OPSEC (Open Platform for Security) und mindestens einen der Standards PKCS#12, CAPI und Entrust unterstützt.

Mit Endpoint Security Client können Sie Check Point-Zertifikate erstellen oder erneuern und Entrust-Zertifikate verwalten.

Verwalten von Entrust-Zertifikaten

Endpoint Security Client umfasst Entrust-Zertifikate. Sie können auf Wunsch mit Entrust Entelligence Zertifikate erstellen und wiederherstellen. Wenn Sie Zertifikate mit Entrust verwalten, stellt der Client gegebenenfalls automatisch eine Verbindung zur Entelligence-Benutzeroberfläche her.

Bevor Sie beginnen, sollten Sie sich vergewissern, dass Ihr Administrator Ihnen eine Referenznummer und einen Autorisierungscode bereitgestellt hat. Diese benötigen Sie, um den Vorgang abzuschließen.

So verwenden Sie ein Entrust-Zertifikat für die Authentifizierung:

Zuerst aktivieren Sie Entrust Entelligence:

1. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.
2. Deaktivieren Sie auf der Registerkarte **Zertifikate** das Kontrollkästchen **Don't use Entrust Entelligence** (Entrust Entelligence nicht verwenden).

Als zweiten Schritt initiieren Sie das Entrust-Zertifikat:

1. Klicken Sie auf der Registerkarte **Zertifikate** auf **Select INI file** (INI-Datei auswählen), suchen Sie die `entrust.ini`-Datei und klicken Sie auf **Öffnen**.
2. Die `entrust.ini`-Datei ist standardmäßig in Ihrem Windows-Verzeichnis (beispielsweise C:\Windows) gespeichert.
3. Klicken Sie auf **Configure INI file** (INI-Datei konfigurieren).
4. Das Fenster **Configure Entrust.INI** (Entrust.INI konfigurieren) wird angezeigt.
5. Geben Sie folgende Informationen an:
6. Hostname oder IP-Adresse des CA-Managers und dessen Portnummer. Die Standard-Portnummer ist 709.
7. Hostname oder IP-Adresse des LDAP-Servers und dessen Portnummer. Die Standard-Portnummer ist 389.
8. Klicken Sie auf **OK**.

Als dritten Schritt erstellen Sie das Entrust-Zertifikat:

1. Klicken Sie auf der Registerkarte **Zertifikate** im Bereich Entrust Certificates (Entrust-Zertifikate) auf **Create** (Erstellen).
2. Das Fenster **Create User** (Benutzer erstellen) wird angezeigt.
3. Klicken Sie auf **Save to File** (In Datei speichern). Suchen Sie dann das Verzeichnis, in dem das Zertifikat gespeichert werden soll.

4. Geben Sie ein Kennwort für Ihr Profil an, und bestätigen Sie es. Das Kennwort muss folgenden Entrust-Spezifikationen entsprechen:
5. Mindestens acht Zeichen lang
6. Mindestens ein Großbuchstabe oder eine Zahl
7. Mindestens ein Kleinbuchstabe
8. Keine langen Zeichenfolgen sich wiederholender Zeichen
9. Keine langen Teilzeichenfolgen des Benutzernamens
10. Geben Sie Ihre Profilparameter an. Dazu geben Sie die **Reference Number** (Referenznummer) und den **Authorization code** (Autorisierungscode) ein, die Sie von Ihrem SystemAdministrator erhalten haben.
11. Klicken Sie auf OK.
12. Klicken Sie im Bestätigungsfenster, das angezeigt wird, erneut auf OK.

Verwalten von Check Point Zertifikaten

Ihr SystemAdministrator kann Sie dazu auffordern, ein neues Check Point-Zertifikat zu erstellen. Sie können ein Check Point-Zertifikat entweder als PKCS#12-Datei (Public-Key Cryptography Standard #12) oder als Hardware- bzw. Software-Token (CAPI) speichern. Besprechen Sie mit Ihrem SystemAdministrator, wie Sie das Zertifikat speichern sollen.

Bevor Sie beginnen, erfragen Sie folgende Informationen bei Ihrem Administrator:

- Zertifikatformat, das Sie verwenden sollen
- Zertifikatregistrierungsschlüssel
- IP-Adresse (oder Hostname) des VPN-Gateway

Erstellen einer PKCS#12-Datei für ein Check Point-Zertifikat

Falls Sie von Ihrem SystemAdministrator dazu aufgefordert wurden, das Zertifikat als PKCS#12-Datei zu speichern, befolgen Sie die Anweisungen in diesem Abschnitt.

So erstellen Sie eine PKCS#12-Datei:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Klicken Sie auf der Registerkarte **Zertifikate** auf **Create Certificate** (Zertifikat erstellen).

Das Fenster Check Point (Check Point-Zertifikat) wird angezeigt.

3. Wählen Sie **Store as a file (PKCS #12)** (Als Datei speichern (PKCS #12)) aus. Klicken Sie auf **Weiter**.
4. Geben Sie die IP-Adresse oder den Hostnamen der Verbindungs-Site sowie den Registrierungsschlüssel an. Klicken Sie auf **Weiter**.
5. Geben Sie ein Kennwort an, das mit dem Zertifikat verwendet werden soll, und bestätigen Sie es. Klicken Sie auf **Weiter**.
6. Klicken Sie im Bestätigungsfenster, das angezeigt wird, auf **Beenden**.

Erstellen eines CAPI-Token für ein Check Point-Zertifikat

Falls Sie von Ihrem SystemAdministrator dazu aufgefordert wurden, das Zertifikat als Hardware- oder Software-Token zu speichern, befolgen Sie die Anweisungen in diesem Abschnitt.

Bevor Sie beginnen, sollten Sie sich vergewissern, dass Ihr Administrator angegeben hat, welcher Cryptographic Service Provider (CSP) verwendet werden soll. Für einige CSPs ist spezielle Hardware erforderlich (beispielsweise ein Token-Leser bzw. -Generator), für andere hingegen nicht. Endpoint Security kann mit den von Windows bereitgestellten CSPs verwendet werden und Check Point stellt die Internal Certificate Authority (ICA) (Interne Zertifizierungsstelle des SicherheitsGateway als CSP bereit.

So erstellen Sie ein Hardware- oder Software-Token:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Klicken Sie auf der Registerkarte **Zertifikate** auf **Create Certificate** (Zertifikat erstellen).

Das Fenster Check Point (Check Point-Zertifikat) wird angezeigt.

3. Wählen Sie **Store on a hardware or software token (CAPI)** (Auf Hardware- oder Software-Token (CAPI) speichern) aus. Klicken Sie auf **Weiter**.
4. Wählen Sie den Cryptographic Service Provider (CSP) für Ihren Zertifikatspeicher aus, und klicken Sie dann auf **Weiter**.



Hinweis - Die Konfigurationsfenster sind von CSP zu CSP verschieden, weshalb es Abweichungen von den verbleibenden Anweisungen geben kann. Details finden Sie in der Dokumentation Ihres CSP.

5. Geben Sie die IP-Adresse oder den Hostnamen der Verbindungs-Site sowie den Registrierungsschlüssel an. Klicken Sie auf **Weiter**.
6. Klicken Sie auf **Security Level**(Sicherheitsstufe), wählen Sie die von Ihrem Administratorangegebene Sicherheitsstufe aus, und klicken Sie auf **Weiter**.
7. Klicken Sie im Fenster, das angezeigt wird, auf **Beenden**.

8. Klicken Sie auf **Ja**.
9. Klicken Sie im Fenster, das angezeigt wird, auf **Beenden**.

Speichern von PKCS#12-Dateien im CAPI-Speicher

Wenn Sie die Check Point ICA (Internal Certificate Authority) des Sicherheits-Gateway als CSP verwenden, können Sie anhand dieser Prozedur PKCS#12-Dateien im CAPI-Speicher ablegen.

So legen Sie die PKCS#12-Datei im CAPI-Speicher ab:

1. Doppelklicken Sie auf die Datei mit der Erweiterung p12.
Der Assistent für den Zertifikatimport wird geöffnet.
2. Klicken Sie auf **Weiter**.
Der korrekte Pfad für die zu importierende Datei wird automatisch angezeigt:
3. Klicken Sie auf **Weiter**, und geben Sie das Kennwort für den privaten Schlüssel ein.
Dies ist der Schlüssel, den Sie von Ihrem SystemAdministrator erhalten haben.
 - **Hohe Sicherheit für den privaten Schlüssel aktivieren:** Jedes Mal, wenn der private Schlüssel vom Client verwendet wird, werden Sie zur Eingabe des Kennworts aufgefordert.
 - **Diesen Schlüssel als exportierbar kennzeichnen:** Sie können den Schlüssel sichern oder später übertragen.
4. Klicken Sie auf **Weiter**, und speichern Sie die Datei entweder automatisch oder in einem bestimmten Ordner.
5. Klicken Sie auf **Fertig stellen**, um den Assistenten für den Zertifikatimport zu beenden.

Speichern des Zertifikats an einem anderen Speicherort

Sie oder Ihr Administrator können sich dafür entscheiden, das Zertifikat nicht im CAPI-Speicher abzulegen.

Wenn Sie beispielsweise mehrere Desktop- und Laptop-PCs verwenden, ist es sicherer, das Zertifikat nicht auf unterschiedlichen Computern zu speichern.

Wenn Ihr Laptop-PC einmal gestohlen wird und sich das Zertifikat nicht auf ihm befindet, können Diebe den Client nicht verwenden, um sich mit Ihrem VPN zu verbinden, weil sie das Kennwort nicht kennen, auch wenn Sie die PKCS#12-Datei besitzen. Aus diesem Grund kann Ihr SystemAdministrator sich dafür entscheiden, nicht das im CAPI-Speicher befindliche Zertifikat zu nutzen und das

System so zu konfigurieren, dass Sie sich mit dem **PKCS#12-Zertifikat** direkt authentifizieren. Ist dies der Fall, wird bei dem Verbindungsversuch mit der aktiven Site eine Meldung angezeigt. Navigieren Sie zu dem Ordner, in dem das Zertifikat gespeichert ist.

So speichern Sie das Zertifikat:

1. Speichern Sie das **PKCS#12-Zertifikat** auf einer Disketten- oder USB-Laufwerk.
2. Konfigurieren Sie das Authentifizierungsschema für die Verwendung von Zertifikaten (Eigenschaftsfenster der Site | Registerkarte **Authentifizierung**).
3. Wählen Sie in der Dropdown-Liste **Zertifikat** die Option **Von Datei**.
4. Navigieren Sie zu den auf einem Disketten- oder USB-Laufwerk gespeicherten Zertifikaten.
5. Geben Sie das Kennwort für das Zertifikat ein.
6. Klicken Sie auf **Verbinden**.

Erneuern von Check Point-Zertifikaten

Der Endpoint Security Client fordert Sie kurz vor Ablauf Ihres Check Point-Zertifikats automatisch dazu auf, dieses zu erneuern. Sie können das Zertifikat jedoch auch jederzeit selbst erneuern.

So erneuern Sie ein Zertifikat mit VPN-Einstellungen (RechtsEndpoint Security-VPN):

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Klicken Sie auf der Registerkarte **Zertifikate** auf **Renew Certificate** (Zertifikat erneuern).

Wenn Ihr Zertifikat in Kürze abläuft, zeigt der Client automatisch das Fenster **Check Point-Zertifikat erneuern**.

3. Bestätigen Sie im Feld **Zertifikat** den Speicherort Ihres aktuellen Zertifikats, oder wechseln Sie zum neuen Speicherort.
4. Geben Sie in das Feld **Current password** (Aktuelles Kennwort) das Kennwort zum Öffnen des Zertifikats an.
5. Klicken Sie auf **Weiter**.

Das Fenster **Save Certificate** (Zertifikat speichern) wird angezeigt.

6. Bestätigen Sie den Namen und den Speicherort der Zertifikatdatei.
7. Geben Sie das neue Kennwort in die Felder **Kennwort** und **Kennwort bestätigen** ein.

Ihr Kennwort sollte mindestens sechs Zeichen lang sein, von denen wenigstens vier Zeichen nur ein Mal vorkommen.

8. Klicken Sie auf **Weiter**.

Das Fenster Check Point (Check Point-Zertifikat) wird angezeigt.

9. Klicken Sie dann auf **Fertig**.

Bei Ihrer nächsten Authentifizierung gegenüber einer Site verwendet der Client dieses erneuerte Zertifikat.

So erneuern Sie ein Zertifikat mit VPN-Einstellungen (Check Point Endpoint Connect-VPN):

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Sites** die relevante Site aus und klicken Sie auf **Eigenschaften**.
3. Öffnen Sie die Registerkarte **Einstellungen** und klicken Sie auf **Renew** (Erneuern).
4. Klicken Sie auf die Dropdown-Liste von **Zertifikat** und wählen Sie Ihr Zertifikat aus.

Das Fenster "Creating a New RSA Signature Key" (Erzeugen eines neuen RSA-Signaturschlüssels) erscheint.

5. Klicken Sie auf **OK** und warten Sie, bis das Fenster **Renewal Succeeded** (Erneuerung erfolgreich) erscheint.

Konfigurieren von Profilen und Sites

Eine Site stellt die Organisation dar, zu der Sie eine Verbindung herstellen möchten. In einem Profil sind die Parameter definiert, mit deren Hilfe der Client die Verbindung zu Ihrer Site herstellt.



Hinweis - Profile werden nur durch Rechts-Endpoint Security VPN unterstützt.

Bevor über Endpoint Security VPN eine Verbindung zu einer Site aufgebaut wird, müssen die Informationen zur Struktur der Site abgerufen werden, beispielsweise die Computer und Server, die innerhalb der Organisation verfügbar sind. Der Verbindungsassistent sammelt diese Site-Informationen. Bei der ersten Verbindung, die sich von allen nachfolgenden Verbindungen unterscheidet, wird die Struktur (oder Topologie) der Site abgerufen. Während dieses Vorgangs werden Sie dazu aufgefordert, durch die Bereitstellung eines Zertifikats oder durch ein anderes Verfahren Ihre Identität nachzuweisen. Wenn Sie sich mithilfe eines

Zertifikats authentifizieren, jedoch noch kein Zertifikat von Ihrem SystemAdministrator erhalten haben, werden Sie zur Registrierung aufgefordert. Bei der Registrierung eines Zertifikats durchlaufen Sie den Prozess der Zertifikaterstellung, der von Ihrem SystemAdministrator initiiert wurde. Nachdem eine Site vollständig definiert wurde, sind regelmäßige Verbindungen möglich.

Im Fenster Einstellungen werden Ihre gesamten Verbindungsprofile angezeigt, also entweder die von Ihnen selbst erstellten Profile oder die Profile, die Ihr SystemAdministrator für Sie erstellt hat. Definieren Sie in diesem Fenster die Site und die Authentifizierungsverfahren.

Verwalten von Verbindungsprofilen

In einem Verbindungsprofil sind die Parameter definiert, mit deren Hilfe der Client die Verbindung zu Ihrer Site herstellt. Die meisten Benutzer benötigen nur ein Profil. Falls sich jedoch Ihre Netzwerkumgebung häufig ändert (beispielsweise wenn Sie gelegentlich aus Hotels oder dem Unternehmensnetzwerk eines Partners eine Verbindung herstellen), müssen Sie oder Ihr SystemAdministrator möglicherweise mehrere unterschiedliche Profile erstellen. Bei jedem Profil wird die Verbindung zu der Site etwas anders aufgebaut, z.B. im Office Mode (Büromodus) oder im Hub Mode (Hub-Modus). Der Endpoint Security Client lädt die neuen Profilinformationen automatisch herunter, wenn Sie die Site aktualisieren. Falls Sie über mehrere Profile verfügen, wenden Sie sich an Ihren Administrator, um zu erfahren, welches Sie verwenden sollen.

Die in diesem Abschnitt beschriebenen Funktionen sind nur in der erweiterten Ansicht verfügbar. (Für Details über kompakte bzw. erweiterte Ansicht siehe **Kompakte und erweiterte VPN-Oberflächen** auf Seite [22.](#))

Erstellen von Profilen

Wenn Sie die erweiterte VPN-Ansicht verwenden, werden Sie möglicherweise von Ihrem SystemAdministrator dazu aufgefordert, ein neues Verbindungsprofil für eine bestimmte Site zu erstellen. Beachten Sie, dass Sie nur dann ein neues Verbindungsprofil erstellen können, wenn Sie bereits mindestens eine Site definiert haben.

So erstellen Sie ein neues Verbindungsprofil:

1. Befolgen Sie eine der folgenden Anweisungen:
 - Öffnen Sie VPNI Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.

- Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol, oder doppelklicken Sie darauf, wählen Sie **Verbindung zu VPN herstellen** und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf der Registerkarte **Verbindungen** auf **Neu | Profil**.
Das Fenster **Profile Properties** (Profileigenschaften) wird geöffnet.
 3. Geben Sie einen Profilnamen und eine Beschreibung an.
 4. Wählen Sie in der Dropdown-Liste **Site** eine Site aus.
 5. Wählen Sie Gateway aus der **Gateway**-Dropdown-Liste aus.
 6. Öffnen Sie die Registerkarte **Erweitert**, und wählen Sie alle von Ihrem Administrator angegebenen Konfigurationsoptionen aus.
 7. Klicken Sie auf **OK**, um das Fenster **Profile Properties** (Profileigenschaften) zu schließen, und dann nochmals auf **OK**, um das Fenster **VPN-Einstellungen** zu schließen.

Exportieren und Importieren von Profilen

Sie können vorhandene Profile exportieren (speichern) und importieren. Z. B. wenn Ihr Administratorein Profil erstellt und Sie dazu auffordert, dieses zu importieren.

So exportieren Sie ein Profil:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Verbindungen** eine der folgenden Optionen aus:
 - Wählen Sie das gewünschte Profil aus, und klicken Sie dann auf **Optionen | Export Profile** (Profil exportieren).
 - Klicken Sie mit der rechten Maustaste auf das gewünschte Profil, und wählen Sie **Export Profile** (Profil exportieren) aus.

Das Profil wird als Datei mit der Erweiterung **SRP** gespeichert.

So importieren Sie ein Profil:

- Klicken Sie auf **Neu | Import Profile** (Profil importieren).

Klonen von Profilen

Sie können Profile klonen und diese anschließend ändern und als neue Profile speichern.

So klonen Sie ein Profil:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Verbindungen** eine der folgenden Optionen aus:
 - Wählen Sie das gewünschte Profil aus, und klicken Sie dann auf **Neu | Clone Profile** (Profil klonen).
 - Klicken Sie mit der rechten Maustaste auf das gewünschte Profil, und wählen Sie **Clone Profile** (Profil klonen) aus.

Das Fenster **Profile Properties** (Profileigenschaften) wird angezeigt.

3. Nehmen Sie die gewünschten Änderungen an den Profileigenschaften vor. Ändern Sie z. B. den Namen, die Beschreibung oder das Gateway.
4. Klicken Sie auf **OK**.

Ändern von Profilen

Wenn Sie die erweiterte VPN-Ansicht verwenden und mehrere Profile konfiguriert haben, können Sie das Profil ändern, mit dem Sie eine Verbindung herstellen.



Hinweis - Sie können Profile bei bestehender Verbindung zu einer VPN-Site nicht ändern.

So wechseln Sie Profile:

1. Wenn Sie mit einer VPN-Site verbunden sind, trennen Sie die Verbindung. Führen Sie dazu eine der folgenden Aktionen aus:
 - Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol von Endpoint Security, und wählen Sie **Verbindung zu VPN trennen** aus.
 - Öffnen Sie **VPN**, und klicken Sie auf **Verbindung trennen**.
2. Öffnen Sie das Fenster **VPN Connection** (VPN-Verbindung). Führen Sie dazu eine der folgenden Aktionen aus:
 - Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol von Endpoint Security, und wählen Sie **Verbindung zu VPN herstellen** aus.

- Öffnen Sie VPN, und klicken Sie auf **Verbinden**.

Das Fenster **VPN Connection** (VPN-Verbindung) wird geöffnet.

3. Wählen Sie in der Dropdown-Liste **Location Profile** (Standortprofil) das gewünschte Profil aus.

4. Geben Sie Ihr Kennwort an, und klicken Sie auf **Verbinden**.

Das ausgewählte Profil ist nun das Standardprofil.

Erstellen einer Desktop-Verknüpfung für ein Profil

Sie können eine Desktop-Verknüpfung zum Aufrufen des Fensters **VPN Connection** (VPN-Verbindung) erstellen und so konfigurieren, dass das von Ihnen ausgewählte Profil verwendet wird. Dies ist nur bei Profilen möglich, mit denen ein bestimmtes Gateway angegeben wird (im Gegensatz zu Profilen, die den Standardwert, "Any Gateway") (Beliebiges Gateway) verwenden).

So erstellen Sie eine Verknüpfung für ein Profil:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Verbindungen** eine der folgenden Optionen aus:
 - Wählen Sie das gewünschte Profil aus, und klicken Sie dann auf **Optionen | Create Shortcut** (Verknüpfung erstellen).
 - Klicken Sie mit der rechten Maustaste auf das gewünschte Profil, und wählen Sie **Create Shortcut** (Verknüpfung erstellen) aus.

Sie können jetzt auf die Verknüpfung auf dem Desktop doppel-klicken, um eine VPN-Verbindung zu initiieren.

Anzeigen von Profileigenschaften

Der Client zeigt Profileigenschaften im Fenster **Profile Properties** (Profileigenschaften) an. Dasselbe Fenster erscheint auch, wenn Sie mit dem Klonen eines Profils oder der Erzeugung eines neuen Profils beginnen.

So zeigen Sie Profileigenschaften an:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Klicken Sie auf der Registerkarte **Verbindungen** mit der rechten Maustaste auf das Profil, und wählen Sie **Eigenschaften** aus.

Das Fenster **Profile Properties** (Profileigenschaften) wird angezeigt.

3. Klicken Sie auf eine Registerkarte:

- **Allgemein:** Site-Name, Site-Beschreibung und ausgewähltes Gateway.
- **Erweitert:** Einstellen von Office Mode (Büromodus), Visitor Mode (Gastmodus) und Hub Mode (Hub-Modus) sowie von Verbindungsoptimierungen

Löschen von Profilen

Wenn Sie die erweiterte VPN-Ansicht verwenden, können Sie nicht mehr benötigte Profile löschen.



Hinweis - Sie können nur Profile löschen, die Sie selbst erstellt haben. Von Ihrem NetzwerkAdministrator heruntergeladene Profile können Sie nicht löschen.

So löschen Sie Profile:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Verbindungen** eine der folgenden Optionen aus:
 - Wählen Sie die Site aus, und klicken Sie auf **Löschen**.
 - Klicken Sie mit der rechten Maustaste auf ein Profil, und wählen Sie **Delete Profile** (Profil löschen) aus.
3. Klicken Sie im Bestätigungsfenster auf **Ja**.

Verwalten von VPN-Sites

Vor dem Aufbau einer VPN-Verbindung müssen Sie eine Ziel-Site (VPN-Server oder -Gerät) definieren, zu der die Verbindung hergestellt werden soll. Eine Site-Definition gibt dem Client an, wie die Verbindung zu der VPN-Site herzustellen ist. Während der ersten Verbindung, die sich von allen nachfolgenden Verbindungen unterscheidet, müssen Sie durch Bereitstellen eines Zertifikats oder durch ein anderes Authentifizierungsverfahren Ihre Identität nachweisen. Der Client ruft dann die Struktur (Topologie) der Site ab. Nachdem die Site definiert wurde, sind regelmäßige Verbindungen möglich.

Definieren von Sites

Bevor Sie eine VPN-Verbindung aufbauen können, müssen Sie eine Site definieren. Falls Sie den Client so konfiguriert haben, dass die erweiterte Version der VPN-Oberfläche angezeigt wird, können Sie nach Bedarf weitere Sites definieren. Führen Sie an Hand der Anweisungen in diesem Abschnitt die einzelnen Schritte des Site-Assistenten aus, um eine neue Site zu definieren.

Vergewissern Sie sich, dass Ihr Administrator Ihnen vor dem Definieren einer Site Folgendes bereitstellt:

- Informationen zum Authentifizierungsverfahren (Benutzername und Kennwort, Zertifikat oder Ähnliches) Falls Sie die Absicht haben, für die Authentifizierung ein Zertifikat zu verwenden, sollten Sie das Zertifikat bereits erstellt oder von Ihrem Administrator erhalten haben (siehe **Verwalten von Zertifikaten** auf Seite [25](#)).
- Die IP-Adresse oder der Name des Sicherheits-Gateway, der Fernzugriff auf das Unternehmensnetzwerk gewährt.

Vorbereitung:

Wenn Sie die VPN-Funktion von Endpoint Security zum ersten Mal nutzen und keine Site definiert haben:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **Verbinden**.
2. Klicken Sie im Fenster, das geöffnet wird, auf **Ja**.

Wenn Sie bereits eine VPN-Ziel-Site definiert haben und eine weitere Site definieren möchten:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen** oder **VPN-Optionen**.
2. Öffnen Sie die Registerkarte **Sites**.
3. Befolgen Sie eine der folgenden Anweisungen:
 - Falls Sie sich in der erweiterten Ansicht befinden, klicken Sie auf **Neu | Site**.
 - Falls Sie sich in der kompakten Ansicht befinden, klicken Sie auf **Define Server** (Server definieren).
 - Falls Sie sich auf der Registerkarte **Sites** befinden, klicken Sie auf **Neu**.

Das Fenster des Site-Assistenten wird angezeigt.

Eine Site definieren:

1. Geben Sie die IP-Adresse oder den Hostnamen der VPN-Site an.
2. Wählen Sie **Display Name** (Anzeigename) aus, und geben Sie einen Anzeigenamen an.
3. Klicken Sie auf **Weiter**.

Es dauert einen Moment, bis der Client die Site identifiziert hat.

4. Wählen Sie das Authentifizierungsverfahren aus. Stellen Sie an Hand der nachfolgenden Aktionen die folgenden Optionen ein:
 - **User name and Password** (Benutzername und Kennwort): Klicken Sie auf **Weiter**, um zum Fenster **User Details** (Benutzerdetails) zu gelangen. Geben Sie Ihren Benutzernamen und das Kennwort an, und klicken Sie auf **Weiter**.
 - **Zertifikat**: Klicken Sie auf **Weiter**, um zum Fenster **Certificate Authentication** (Zertifikatauthentifizierung) zu gelangen. Suchen Sie Ihr Zertifikat, wählen Sie es aus, und geben Sie dann das Zertifikatkennwort an. Klicken Sie auf **Weiter**.
 - **SecurID** (SecurID): Klicken Sie auf **Weiter**, um zum Fenster **SecurID Authentication** (SecurID-Authentifizierung) zu gelangen. Wählen Sie **Use Key FOB hard token** (Key FOB-Hardware-Token verwenden), **Use PinPad card** (PinPad-Karte verwenden) oder **Use SecurID Software token** (SecurID-Software-Token verwenden) aus. Klicken Sie auf **Weiter**. Geben Sie die erforderlichen Informationen zum Authentifizierungstyp an. Klicken Sie auf **Weiter**.
 - **Challenge Response** (Antwort auf Rückfrage): Klicken Sie auf **Weiter**, um zum Fenster **Challenge Response** (Antwort auf Rückfrage) zu gelangen. Geben Sie Ihren Benutzernamen ein, und klicken Sie auf **Weiter**.
5. Wählen Sie bei Aufforderung die gewünschte Verbindungseinstellung (**Standard** oder **Erweitert**) aus, und klicken Sie auf **Weiter**.

Nach einer kurzen Wartezeit werden im nächsten Fenster **Please Validate Site** (Bitte Site validieren) der Fingerabdruck Ihres Zertifikats und **Distinguished Names (DN)** angezeigt.

Falls Sie den Fingerabdruck der Site und den DN von Ihrem Administrator erhalten haben, vergleichen Sie diese mit denen in diesem Fenster. Stimmen sie überein, klicken Sie auf **Weiter**.

Das Fenster **Site Created Successfully** (Site erfolgreich erzeugt) wird angezeigt.

6. Klicken Sie dann auf Fertig.

Anzeigen von Site-Eigenschaften

Der Client zeigt Ihnen Site-Eigenschaften wie z. B. die IP-Adresse der Site und das Authentifizierungsverfahren an. Die Informationen im Fenster Site Properties (Site-Eigenschaften) ist in folgende Kategorien unterteilt:

- **Allgemein:** Gibt den Site-Namen, die IP-Adresse der Site und den Zeitpunkt der letzten Site-Aktualisierung an.
- **Authentifizierung:** Hier können Sie das Authentifizierungsverfahren anzeigen oder ändern. Siehe **Ändern von Authentifizierungsverfahren** auf Seite 24.
- **Erweitert:** Aktivieren Sie das NAT-T-Protokoll. Siehe **Aktivieren von Verbindungsoptimierungen** siehe "NAT Traversal Tunneling" auf Seite 53.

So zeigen Sie Site-Eigenschaften an:

1. Öffnen Sie VPNI Grundeinstellungen, und klicken Sie auf VPN-Einstellungen oder VPN-Optionen.
2. Klicken Sie auf der Registerkarte Verbindungen oder Sites mit der rechten Maustaste auf die gewünschte Site (nicht auf das Profil, sondern auf die Site, die das Profil umfasst), und wählen Sie Eigenschaften aus.
Das Fenster Profile Properties (Profileigenschaften) wird angezeigt.
3. Öffnen Sie Allgemein, Authentifizierung oder Erweitert.

Aktualisieren von Sites

Wenn Sie eine Site aktualisieren, laden Sie alle neuen Client-Einstellungen und sämtliche aktualisierten Informationen zu der Site und den zugehörigen Profilen herunter, einschließlich aller neuen Profile, die Ihr Administrator konfiguriert hat. Zum Aktualisieren einer Site muss zunächst eine Verbindung zu der Site bestehen. Falls keine Verbindung besteht und Sie versuchen, die Aktualisierung auszuführen, werden Sie vom Client zum Herstellen einer Verbindung aufgefordert.

So aktualisieren Sie eine Site:

1. Öffnen Sie VPNI Grundeinstellungen, und klicken Sie auf VPN-Einstellungen.
2. Wählen Sie auf der Registerkarte Verbindungen oder Sites eine Site aus und klicken Sie auf Optionen | Update Site.

Wenn Sie bereits mit der Site verbunden sind, zeigt ein Fenster für den Aktualisierungsfortschritt an, ob die Aktualisierung vollständig ist.

Falls Sie nicht verbunden sind, werden Sie vom Client zum Herstellen einer Verbindung aufgefordert. Sie müssen dies tun, um die Aktualisierung abschließen zu können.

Deaktivieren von Sites

Sie können eine Site deaktivieren und zu einem späteren Zeitpunkt wieder aktivieren. Beachten Sie, dass Sie durch die Deaktivierung der Site auch alle zugehörigen Profile deaktivieren.

So deaktivieren Sie eine Site:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Verbindungen** Ihre VPN-Verbindung aus.
3. Befolgen Sie eine der folgenden Anweisungen:
 - Wählen Sie die gewünschte Site aus, und klicken Sie dann auf **Optionen | Disable Site** (Site deaktivieren).
 - Klicken Sie mit der rechten Maustaste auf das gewünschte Profil, und wählen Sie **Disable Site** (Site deaktivieren) aus.

Unter den Symbolen für die Site und die zugehörigen Profile wird ein rotes "x" angezeigt. Es gibt an, dass sie deaktiviert sind.

So aktivieren Sie eine Site wieder:

- Wählen Sie die Site aus, und klicken Sie dann auf **Optionen | Enable Site** (Site aktivieren).
- Klicken Sie mit der rechten Maustaste auf die Site, und wählen Sie **Enable Site** (Site aktivieren) aus.

Löschen von Sites

Sie können nicht mehr benötigte Sites löschen.



Wichtig - Durch das Löschen einer Site löschen Sie auch alle zugehörigen Profile.

So löschen Sie Sites:

1. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf die Registerkarte VPN-Einstellungen | Verbindungen.
2. Trennen Sie Ihre VPN-Verbindung.
3. Befolgen Sie eine der folgenden Anweisungen:
 - Wählen Sie die Site aus, und klicken Sie auf Löschen.
 - Klicken Sie mit der rechten Maustaste auf die Site, und wählen Sie Delete Site (Site löschen) aus.
4. Klicken Sie im Bestätigungsfenster, das angezeigt wird, auf Ja.

Herstellen und Trennen von Verbindungen

In diesem Abschnitt wird erläutert, wie Sie eine Verbindung zu einer VPN-Site herstellen und diese anschließend wieder trennen. Für diese Anweisungen wird vorausgesetzt, dass Sie bereits mindestens eine Site definiert haben.

So stellen Sie eine Verbindung zu einer bestehenden Site her:

- Wenn diese Option zur Verfügung steht, klicken Sie auf Quick Connect (schnelle Verbindung). Sie sind mit vordefinierten Anmeldeinformationen verbunden.
1. Wenn diese Option nicht zur Verfügung steht, führen Sie eine der folgenden Aktionen aus:
 - Klicken Sie mit der rechten Maustaste auf das Symbol von Endpoint Security in der Taskleiste, und wählen Sie Verbindung zu VPN herstellen aus.
 - Klicken Sie unter Endpoint Security | VPN auf Verbinden.

Das Fenster VPN Connection (VPN-Verbindung) wird geöffnet. Die Felder, die im Fenster angezeigt werden, variieren je nach Ihrem Authentifizierungsverfahren. Wenn Sie sich beispielsweise mit Zertifikaten authentifizieren, wird der Pfad des Zertifikats angezeigt, und Sie werden dazu aufgefordert, Ihr Kennwort einzugeben.

2. Geben Sie die entsprechenden Informationen an, und klicken Sie auf Verbinden.

Endpoint Security zeigt ein Fenster mit einer Fortschrittsanzeige und der Information an, ob die Verbindung hergestellt wurde.

So trennen Sie die Verbindung:

1. Befolgen Sie eine der folgenden Anweisungen:
 - Klicken Sie mit der rechten Maustaste auf das Symbol von Endpoint Security in der Taskleiste, und wählen Sie **Verbindung zu VPN trennen** aus.
 - Öffnen Sie unter Endpoint Security **VPN | Trennen**.
Ein Bestätigungsfenster wird angezeigt.
2. Klicken Sie auf **Ja**.

Verbindungsstatus

Sie können verschiedene Arten von Informationen zum Verbindungsstatus anzeigen.

So zeigen Sie Informationen zum Verbindungsstatus an:

- Öffnen Sie **VPN**: Hier können Sie den aktuellen Verbindungsstatus, den Namen des aktiven Profils, die Verbindungsdauer und die bis zur erneuten Authentifizierung verbleibende Zeit anzeigen.
- Öffnen Sie **VPN|Aktivität**: Hier können Sie Details zur Komprimierung und Dekomprimierung von IP-Paketen anzeigen.
- Öffnen Sie **VPN**, und klicken Sie auf den Link **Verbindungsdetails**: Hier können Sie Verbindungsdetails anzeigen.

Grundlegendes zu Verbindungsdetails - Rechts-VPN

Endpoint Security Client stellt die folgenden Kategorien von Informationen zur aktuellen Verbindung bereit, wenn Ihr VPN lautet wie folgt: SecureClient (Rechts-Check Point VPN).

Table 0- 2 Rechts-VPN, Verbindungsdetails

Informationstyp	Beschreibung
Status Summary (Statusübersicht):	Verbindungsstatus des Clients, IP-Adresse des Gateway, IP-Adresse des aktuellen Computers.
Verbindungen	Name, IP-Adresse, Site-Name und Tunneleigenschaften jedes verfügbaren Gateway. Das aktive Gateway ist designiert als („primäres Gateway“).

Gateway-Informationen	Weitere Gateway-Informationen
UDP Encapsulation (UDP-Kapselung):	Versetzt Endpoint Security Client in die Lage, durch Hide NAT-Geräte verursachte Probleme zu beseitigen.
Visitor Mode (Gastmodus):	Versetzt Endpoint Security Client in die Lage, eine Verbindung über ein Gateway herzustellen, bei dem Verbindungen auf Port 80 oder 443 beschränkt sind.
Aktivieren des Office Mode (Büromodus)	Durch den Office Mode (Büromodus) werden Konflikte in Remote-Netzwerken verhindert, da sicher gestellt wird, dass der Client eine eindeutige IP-Adresse vom Gateway erhält.
Tunnel Active (Tunnel aktiv):	Gibt an, ob der VPN-Tunnel geöffnet ist.
IP Compression (IP-Komprimierung):	Gibt an, ob Daten für langsame Links wie zum Beispiel Einwahlverbindungen komprimiert werden.
IKE over TCP (IKE über TCP):	Gibt an, ob die Tunnelverhandlung über TCP stattfindet oder nicht (wenn nicht, findet sie über UDP statt). Für komplexen IKE aktivieren.
Tunnel MTU Properties (Eigenschaften von Tunnel-MTU):	Hier wird die aktuelle maximale MTU angezeigt. Wenn der Client über mehrere Router mit einer Site kommuniziert, ist es die kleinste MTU aller Router, die von Bedeutung ist.
Computer (Computer):	Der Verbindungsstatus des aktuellen Computers und weitere Informationen zur Verbindung.
Active Connection Settings (Einstellungen der aktiven Verbindung):	Zusammenfassung des aktuellen Profils, einschließlich: Site, zu der eine Verbindung hergestellt werden soll Gateway, Hostname, Protokoll-Spezifikationen
Name	Name des Verbindungsprofils, wie er im Fenster VPN Connection (VPN-Verbindung) angezeigt wird. Hierbei kann es sich um eine IP-Adresse handeln.
Beschreibung	Beschreibender Name für das Profil, der weitere Informationen angibt.
Site	Name der Site, zu der eine Verbindung hergestellt werden soll.
Profil Gateway	Name des im Verbindungsprofil angegebenen Gateway.
Ausgewähltes Gateway	Das gegenwärtig für die Verbindung ausgewählte Gateway ist möglicherweise nicht mit dem im Verbindungsprofil definierten Gateway identisch.

Name des im Verbindungsprofil definierten Gateway.	Name des definierten Gateway.
Support Office mode (Büromodus unterstützen):	Gibt an, ob der Office Mode (Büromodus) unterstützt wird.
Support IKE over TCP (IKE über TCP unterstützen):	Gibt an, ob die Tunnelverhandlung über TCP anstelle von UDP stattfindet, um die Paketfragmentierung zu vermeiden.
Force UDP Encapsulation (UDP-Kapselung erzwingen):	Gibt an, ob die UDP-Kapselung eingesetzt wird, um Probleme zu beseitigen, die durch Hide NAT-Geräte verursacht werden. Hide NAT-Geräte unterstützen die Paketfragmentierung nicht.
Visitor Mode (Gastmodus):	Gibt an, ob der Visitor Mode (Gastmodus) aktiv ist.
Gesamten Datenverkehr über Gateway weiterleiten; Hub Mode (Hub-Modus)	Gibt an, ob der Hub Mode (Hub-Modus) aktiv ist.
Tunnel MTU Discovery (Ermittlung von Tunnel-MTU):	Gibt an, ob der Prozess, der die MTU vom Endpoint Security zum Gateway ermittelt, aktiv ist.

Grundlegendes zu Verbindungsinformationen - Endpoint Connect VPN

Der Endpoint Security Client bietet folgende Informationen, wenn Sie Endpoint Connect als VPN nutzen.

Details, Registerkarte	Beschreibung
Name	Name des VPN-Site Gateway, mit dem Sie aktuell verbunden sind.
IP-Adresse	IP-Adresse der VPN-Site.
Letzte Verbindung	Tag, Datum und Uhrzeit der letzten Verbindung mit dieser Site.
Letzte IP-Adresse im Büromodus	IP-Adresse des Büromodus von VPN Gateway, sofern relevant.

Grundlegendes zu Verbindungseinstellungen - Endpoint Connect VPN

Einstellungen, Registerkarte	Beschreibung
Immer verbinden	Wenn Ihr Client das Ändern dieser Option gestattet, wählen Sie Immer verbinden , um automatisch eine Verbindung mit dem aktiven VPN herzustellen, wenn dies möglich ist.
VPN-Kanalisierung	Wenn Ihr Client das Ändern dieser Option erlaubt, wählen Sie Gesamten Verkehr verschlüsseln und an Gateway leiten , um die Funktion zur VPN-Kanalisierung für den gesamten Verkehr dieses Clients zu verwenden.
Authentifizierung	Wählen Sie in der Dropdown-Liste ein Authentifizierungsverfahren aus.

Aktivieren der Protokollierung

Möglicherweise werden Sie zu Fehlerbehebungszwecken von Ihrem System Administrator gebeten, ein Berichtsprotokoll zu erstellen. Das Berichtsprotokoll enthält Site-spezifische Informationen und sollte streng vertraulich behandelt werden. Senden Sie den Bericht nur an Ihren SystemAdministrator oder an eine andere autorisierte Instanz.

So aktivieren Sie die Protokollierung:

1. Öffnen Sie VPN | Grundeinstellungen, und klicken Sie auf VPN-Einstellungen oder VPN-Optionen.
2. Wählen Sie auf der Registerkarte Erweitert **Enable Logging** (Protokollierung aktivieren) aus.

Senden von Protokollen:

1. Klicken Sie auf der Registerkarte Erweitert auf **Save Logs** (Protokolle speichern) oder auf **Collect Logs** (Protokolle sammeln).

Wenn der Administrator eine E-Mail-Adresse für die Protokolle vorkonfiguriert hat, öffnet sich Ihr standardmäßig eingestelltes E-Mail-Programm mit eingetragener Supportadresse und als CAB-Datei angehängten Protokollen.

Wenn folgende Meldung erscheint (Send this report only to your system Administrator.) (Senden Sie den Bericht nur an Ihren Systemadministrator), klicken Sie auf OK.

2. Bitte warten, während die Protokolle verbunden werden. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf OK.

Das Verzeichnis, in dem die Protokolle gespeichert sind, wird geöffnet.

3. Senden Sie die CAB- oder TGZ-Datei an den Administrator.

Konfigurieren von Verbindungsoptionen

In diesem Abschnitt werden verschiedene Verbindungs- und Anmeldungsoptionen beschrieben.



Hinweis - In der kompakten Version der VPN-Oberfläche sind die Optionen Auto-Connect (Autom. Verbindung), Secure Domain Logon (Sichere Anmeldung über Domäne) und Auto Local Logon (Autom. lokale Anmeldung) nicht verfügbar.

Auto-Connect (Autom. Verbindung)

Diese Option ist nur in RechtsEndpoint Security-VPN verfügbar.

Wenn die Option **Auto-Connect** (Autom. Verbindung) ausgewählt ist, werden Sie bei Ihrem ersten Zugriffsversuch auf ein privates Netzwerk wie das Unternehmens-Internet dazu aufgefordert, eine VPN-Verbindung herzustellen. Hierdurch sparen Sie Zeit, da Sie nicht durch Endpoint Security navigieren und die Verbindung selbst initiieren müssen.

Im Modus "Auto-Connect" (Autom. Verbindung) werden Sie vom Client jedes Mal, wenn dieser für Ihr Unternehmensnetzwerk oder eine Intranet-Site bestimmten Datenverkehr erkennt, zum Herstellen einer VPN-Verbindung aufgefordert.

- Wenn Sie die Verbindung herstellen, verschlüsselt der Client den Datenverkehr zu der Site.
- Stellen Sie keine Verbindung her, so fordert der Client Sie dazu auf anzugeben, wie lange gewartet werden soll, bevor Sie erneut daran erinnert werden, eine Verbindung aufzubauen. Während dieses Zeitraums wird Datenverkehr an die Site unverschlüsselt gesendet. Falls die Site jedoch so konfiguriert ist, dass sämtlicher unverschlüsselter Datenverkehr verworfen wird, können Sie keine Daten an Server hinter dem Gateway der Site übertragen.

- Falls der Office Mode (Büromodus) ebenfalls aktiviert ist, müssen Sie die Verbindung nach erfolgreicher Verbindung im Modus "Auto-Connect" (Autom. Verbindung) erneut initiieren.

So aktivieren Sie "Auto-Connect" (Autom. Verbindung):

1. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.
2. Wählen Sie auf der Registerkarte Optionen das Kontrollkästchen Enable Auto-Connect (Autom. Verbindung) aus, und klicken Sie auf OK.

Das Fenster Enable Auto Connect (Autom. Verbindung aktivieren) wird angezeigt.

3. Wählen Sie eine Option für einen erneuten Start aus.
4. Klicken Sie auf OK.

Secure Domain Logon (Sichere Anmeldung über Domäne)

Diese Option ist nur in RechtsEndpoint Security-VPN verfügbar.

In einer Windows-Umgebung gehört Ihr Konto eventuell zu einer Domäne, die von einem Domänen-Controller gesteuert wird (ein Computer, der Netzwerkbenutzern und -Computern den Microsoft Active Directory-Dienst bereitstellt.) Secure Domain Login (Sichere Anmeldung über Domäne, SDL) ist nützlich, wenn sich der Domänen-Controller hinter der Firewall Ihrer Site befindet.

Wenn Sie versuchen, eine VPN-Verbindung zu einer Windows-Domäne herzustellen, sendet der Client Ihre Anmeldedaten zur Verifizierung an den Domänen-Controller. Wenn Sie SDL aktivieren, stellt der Client die VPN-Verbindung *vor* der Übertragung von Daten zum und vom Domänen-Controller her.

So aktivieren Sie "Secure Domain Logon" (Sichere Anmeldung über Domäne):

1. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.
2. Wählen Sie auf der Registerkarte Optionen Enable Secure Domain Logon (Sichere Anmeldung über Domäne) aus, und klicken Sie auf OK.

Auto Local Logon (Autom. lokale Anmeldung)

Diese Option ist nur in RechtsEndpoint Security-VPN verfügbar.

Wenn Sie sich mit einem Benutzernamen und einem Kennwort (und nicht mit einem Zertifikat) bei einer VPN-Site anmelden, können Sie Ihre Anmeldung automatisieren, indem Sie die Option Auto Local Logon (Autom. lokale Anmeldung) aktivieren.

Falls Sie sowohl **Auto Local Logon** (Autom. lokale Anmeldung) als auch **Auto-Connect** (Autom. Verbindung) aktivieren, stellt der Client bei Ihrem ersten Zugriffsversuch auf eine Site, für die eine verschlüsselte Datenübertragung erforderlich ist (also bei Datenverkehr zur VPN-Site), automatisch eine VPN-Verbindung her. Dies ist für unbeaufsichtigte Computer praktisch, die vielen Endbenutzern als Terminal dienen.

So aktivieren Sie "Auto Local Logon" (Autom. lokale Anmeldung):

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen**.
2. Wählen Sie auf der Registerkarte **Optionen** **Enable Auto Local Logon** (Autom. lokale Anmeldung aktivieren) aus, und klicken Sie auf **Auto Local Logon Options** (Autom. lokale Anmeldung - Optionen).

Das Fenster **Auto Local Logon** (Autom. lokale Anmeldung) wird angezeigt.

3. Geben Sie Ihren Windows-Benutzernamen, Ihr Windows-Kennwort, Ihren VPN-Benutzernamen und Ihr VPN-Kennwort an, und klicken Sie dann auf **OK**.

Es wird die Meldung angezeigt, dass Ihre Änderung nach dem nächsten Neustart wirksam wird.

4. Wenn das Fenster geschlossen wird, klicken Sie auf **OK**, um das Fenster **VPN-Einstellungen** zu schließen.

Verbindung immer herstellen

Diese Option steht nur im Check Point Endpoint Connect VPN zur Verfügung.

So halten Sie die Verbindung zur aktiven Site immer aufrecht:

1. Öffnen Sie **VPN | Grundeinstellungen**, und klicken Sie auf **VPN Optionen**.

Das Optionsfenster wird geöffnet.

2. Öffnen Sie die Registerkarte **Sites**.

3. Wählen Sie eine Site aus, und klicken Sie auf **Eigenschaften**.

Das Eigenschaftsfenster wird geöffnet.

4. Wählen Sie die Option zum ständigen Aktivieren der Verbindung, und klicken Sie auf **OK**.

Herstellen einer Verbindung über einen Hotspot.

Ihr Unternehmen oder eine getrennte Richtlinie lässt möglicherweise nicht automatisch einen Zugriff auf Ihr Netzwerk über einen Wireless-Hotspot in einem Hotel oder an einem anderen öffentlichen Ort zu. Eventuell gestattet die Richtlinie es Ihnen aber, dass Sie diese Einschränkung teilweise aufheben, um einen Hotspot zu registrieren. Diese Aufhebung gilt nur temporär und weist folgende Beschränkungen auf:

- Nur die Ports 80, 8080 und 443 werden geöffnet. Diese Ports werden in der Regel für die Hotspot-Registrierung verwendet.
- Während der Registrierung des Hotspot sind maximal fünf IP-Adressen zulässig.
- Falls eines der folgenden Ereignisse eintritt, werden die Ports 80, 8080 und 443 geschlossen:
 - Erfolgreiche Verbindung zum Netzwerk
 - Ablauf von zehn Minuten
 - Drei fehlgeschlagene Verbindungsversuche

So aktivieren Sie die Hotspot-Registrierung:

1. Befolgen Sie eine der folgenden Anweisungen:

- Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol, und wählen Sie **Bei Hotspot/Hotel registrieren** aus.
- Öffnen Sie das Fenster **Verbinden**, und klicken Sie auf **Optionen**. Wählen Sie dann **Bei Hotspot/Hotel registrieren** aus.

Es wird eine Meldung angezeigt, der Sie den für die Registrierung zulässigen Zeitraum entnehmen können.

2. Stellt eine Verbindung zum Internet her.



Falls die Option **Bei Hotspot/Hotel registrieren** nicht verfügbar ist, wurde diese Funktion von Ihrem NetzwerkAdministrator deaktiviert.

Aktivieren des Office Mode (Büromodus)

Im Office Mode (Büromodus) weist das Gateway Ihrem Computer eine temporäre IP-Adresse zu, bei der sichergestellt ist, dass kein Konflikt zu einer anderen IP-Adresse an der Site besteht. Die Zuweisung erfolgt nach der Authentifizierung und

bleibt für die Dauer der Verbindung gültig. Diese Funktion beseitigt bestimmte Verbindungsprobleme.

Der Office Mode (Büromodus) kann durch ein Profil aktiviert werden, das Ihr Administrator dem Client bereitstellt. Sie können ihn alternativ auch manuell aktivieren.



Hinweis - Wenn der Office Mode (Büromodus) gemeinsam mit dem Modus „Auto-Connect“ (Autom. Verbindung) aktiviert wird, müssen Sie die Verbindung nach erfolgreicher Verbindung im Modus „Auto-Connect“ (Autom. Verbindung) erneut-initiieren.

So aktivieren Sie den Office Mode (Büromodus):

1. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.
2. Klicken Sie auf der Registerkarte Verbindungen mit der rechten Maustaste auf das Profil, und wählen Sie Eigenschaften aus.

Das Fenster Profile Properties (Profileigenschaften) wird angezeigt.

3. Klicken Sie auf die Registerkarte Erweitert, wählen Sie Office Mode (Büromodus) aus, und klicken Sie auf OK.

Aktivieren des Hub Mode (Hub-Modus)

Im Hub Mode (Hub-Modus) kann Endpoint Security das Site-Gateway als Router verwenden. Der Datenverkehr von Endpoint Security VPN wird nicht an die interne Site, sondern an ein anderes Gateway weitergeleitet. Wenn sich Ihr SystemAdministrator zur Verwendung von Hub Mode (Hub-Modus) entscheidet, kann es sein, dass er Sie dazu auffordert, ihn manuell zu aktivieren.

So aktivieren Sie den Hub Mode (Hub-Modus):

1. Öffnen Sie VPN | Grundeinstellungen.
2. Wenn Sie die Schaltfläche VPN-Einstellungen sehen:
 - a. Klicken Sie auf VPN-Einstellungen.
 - b. Wählen Sie auf der Registerkarte Verbindungen ein Profil aus und klicken Sie auf Eigenschaften.
 - c. Öffnen Sie die Registerkarte Erweitert.
 - d. Wählen Sie Route all traffic through Gateway (Gesamten Datenverkehr über Gateway weiterleiten), und klicken Sie dann auf OK.
3. Wenn Sie die Schaltfläche VPN-Optionen sehen:

- a. Klicken Sie auf **VPN-Optionen**.
- b. Wählen Sie auf der Registerkarte **Sites** eine Site aus und klicken Sie auf **Eigenschaften**.
- c. Öffnen Sie die Registerkarte **Einstellungen**.
- d. Wählen Sie **Encrypt all traffic and route to Gateway** (Gesamten Datenverkehr verschlüsseln und zu Gateway weiterleiten), und klicken Sie dann auf **OK**.



Hinweis - Der Administrator muss das SicherheitsGateway so konfigurieren, dass es als ein Hub arbeitet, d. h. eine Netzwerkanwendung definieren, die den folgenden Bereich umfasst: 0.0.0.1 > 255.255.255.254.

Proxy-Einstellungen (Visitor Mode (Gastmodus))

Falls Sie von einem Remote-Standort, beispielsweise aus einem Hotel oder den Räumlichkeiten eines Kunden, über das Internet eine Verbindung zu Ihrem Unternehmen herstellen, ist die Verbindung möglicherweise auf einen Webzugriff über die Standardports für HTTP-Datenverkehr begrenzt. Dies sind gewöhnlich Port 80 für HTTP und Port 443 für HTTPS. Der Remote-Client muss über Port 500 eine IKE-Verhandlung durchführen oder IPSec-Pakete senden (statt der üblichen TCP-Pakete). Daher ist es nicht möglich, auf die herkömmliche Weise einen VPN-Tunnel einzurichten. Dieses Problem wird mit dem Visitor Mode (Gastmodus) (auch als *TCP Tunneling* bekannt), über einen Proxyserver gelöst.

Bevor Sie Proxy-Einstellungen konfigurieren, wenden Sie sich an Ihren SystemAdministrator, um einen gültigen Benutzernamen und ein Kennwort für den Proxyzugriff zu erhalten. Möglicherweise benötigen Sie auch die IP-Adresse und Portnummer des Proxyservers.

So konfigurieren Sie Proxy-Einstellungen:

1. Öffnen Sie **VPN| Grundeinstellungen**, und klicken Sie auf **VPN-Einstellungen** oder **VPN-Optionen**.
2. Befolgen Sie eine der folgenden Anweisungen:
 - Klicken Sie auf **VPN-Einstellungen**. Klicken Sie auf der Registerkarte **Optionen** auf **Configure Proxy Settings** (Proxy-Einstellungen konfigurieren).
 - Von **VPN-Optionen**: Klicken Sie auf der Registerkarte **Erweitert** auf **Proxy Settings** (Proxy-Einstellungen).
3. Konfigurieren Sie die Proxy-Einstellungen.

- **No proxy / transparent proxy** (Kein Proxy/Transparenter Proxy): Standardeinstellung.
 - **Detect proxy from Internet Explorer settings:** (Proxy an Hand der Internet Explorer-Einstellungen erkennen) Proxy an Hand der Internet Explorer-Einstellungen erkennen. Achten Sie vor der Auswahl dieser Einstellung darauf, dass die Einstellungen manuell definiert sind: Vergewissern Sie sich in Microsoft Internet Explorer unter > Internetoptionen > Registerkarte Verbindungen > LAN-Einstellungen, dass die Option "Proxyserver für diese Verbindung verwenden" ausgewählt ist. Falls die Option Automatische Suche der Einstellungen oder Automatisches Konfigurationsskript verwenden ausgewählt ist, kann der Client nicht die Proxy-Einstellungen von Microsoft Internet Explorer ermitteln.
 - **Manually define proxy:** (Proxy manuell definieren) Wenn die Proxy-Einstellungen nicht automatisch erkannt werden können, müssen Sie die Einstellungen von Microsoft Internet Explorer unter Umständen an Hand der von Ihrem SystemAdministrator bereitgestellten Anweisungen, IP-Adresse und Portnummer konfigurieren.
4. Geben Sie im Abschnitt **Proxy Authentication** (Proxy-Authentifizierung) den Benutzernamen und das Kennwort für die Proxy-Authentifizierung an.
 5. Klicken Sie auf OK.

DFÜ-Support

Sie können die Option zum Konfigurieren und Verwenden von DFÜ-Verbindungen mit Endpoint Security verwenden, wenn Sie über den Endpoint Connect VPN-Client verfügen.

Ist kein Netzwerk verfügbar, wenn Sie versuchen, sich mit einer Site zu verbinden, und wurde keine DFÜ-Verbindung konfiguriert, zeigt der Endpoint Connect Client eine Meldung an:

Verbindung fehlgeschlagen

Kein Netzwerk gefunden

Klicken Sie hier, um DFÜ-Verbindungen zu aktivieren

- Klicken Sie auf den Link, um den Assistenten für neue Verbindungen zu öffnen und eine DFÜ-Verbindung zu konfigurieren.
- Ist bereits eine DFÜ-Verbindung definiert, klicken Sie auf den Link, um die Verbindung herzustellen.
- Sind mehrere DFÜ-Verbindungen definiert, wird eine Liste angezeigt. Wählen Sie eine Verbindung aus, die Endpoint Connect wählen soll.

- Sind die Optionen für Transparentes Netzwerk und Interface-Roaming aktiviert und befindet sich das VPN im Status des erneuten Verbindungsaufbaus, zeigt Endpoint Connect eine Meldung für den erneuten Verbindungsaufbau mit dem Link zum Aktivieren der DFÜ-Verbindung an.

Erweiterte Konfigurationsoptionen

Wenn Sie die erweiterte Version der VPN-Oberfläche verwenden, stellt der Client die erweiterten Konfigurationsoptionen bereit.

Deaktivieren von Popup-Meldungen

Wenn Endpoint Security VPN von der Site getrennt wird und die Option Auto-Connect (Autom. Verbindung) aktiviert ist, werden Sie jedes Mal, wenn Endpoint Security VPN an die Site gerichteten Datenverkehr erkennt, durch eine Popup-Meldung zum Herstellen einer Verbindung aufgefordert. Diese Popup-Meldung kann deaktiviert werden.

Wenn Sie beispielsweise festlegen, dass Popup-Meldungen für 60Minuten deaktiviert werden, wird der gesamte Datenverkehr zu der Site während dieser 60Minuten entweder verworfen oder unverschlüsselt gesendet. Nach Ablauf der 60Minuten werden Sie wieder jedes Mal, wenn Endpoint Security VPN an die Site gerichteten Datenverkehr erkennt, zum Herstellen einer Verbindung aufgefordert.

So deaktivieren Sie Popup-Meldungen:

1. Klicken Sie mit der rechten Maustaste auf das Taskleistensymbol von Endpoint Security.
2. Wählen Sie im Popup-Menü die Optionen VPN-Optionen/Popups für autom. Verbindung deaktivieren aus.

Das Fenster Suspend Popup Messages (Popup-Meldungen deaktivieren) wird angezeigt.

3. Wählen Sie die gewünschte Option für die Deaktivierung von Popup-Meldungen aus.
4. Klicken Sie auf OK.

NAT Traversal Tunneling

Network Address Translation (Übersetzung von Netzwerkadressen) stellt unterschiedliche Arten von Sicherheiten bereit, die sich von dem VPN- und dem

IPSec-VPN-Protokoll unterscheiden. Um NAT mit Ihrem VPN zu verwenden, müssen Sie Ihren VPN Client so konfigurieren, dass er NAT-T unterstützt. Dies muss in Zusammenarbeit mit dem Administrator der Firewall Gateway erfolgen, da NAT-T-Ports und Optionen sowohl in Ihren Client als auch in dem Gateway konfiguriert sein müssen, damit sie sich gegenseitig unterstützen.

NAT Traversal Aktivieren:

1. Öffnen Sie VPN | Grundeinstellungen , und klicken Sie auf VPN-Einstellungen.
2. Klicken Sie auf der Registerkarte Verbindungen mit der rechten Maustaste auf das Profil, und wählen Sie Eigenschaften aus.

Das Fenster Profile Properties (Profileigenschaften) wird angezeigt.

3. Öffnen Sie die Registerkarte Erweitert und wählen Sie Connectivity enhancements (Verbindungsoptimierungen) aus.
4. Wählen Sie Use NAT traversal tunneling (NAT Traversal Tunneling verwenden) aus.

Ihr Administrator muss das aktivierte NAT-T auf dem Gateway unterstützen, und den UDP-Port 4500 für die VPN-Sitzung öffnen. In der Firewall muss ein NAT-Gerät definiert werden.

NAT-T unterstützt nicht den IKE Aggressive Mode.

5. Wählen Sie relevante Optionen aus, um Probleme in Zusammenhang mit großen Paketen zu lösen.
 - IKE over TCP (IKE über TCP): Durch TCP-Pakete wird das Problem der Erstellung großer UDP-Pakete während IKE-Phase 1 behoben. Diese Option ist relevant, wenn der VPN IKE-Protokolle verwendet. Der Administrator muss die Unterstützung von IKE über TCP aktivieren.
 - Force UDP Encapsulation (UDP-Kapselung erzwingen): Das Problem großer UDP-Pakete wird durch Verpacken derselben in IPSec-Überschriften gelöst. Der Administrator muss Port 2746 für Quelle und Ziel aktivieren.
6. Klicken Sie auf OK.

Befehlszeilenoptionen

Check Point Endpoint Connect VPN Client kann auch über die Befehlszeile ausgeführt werden.

So verwenden Sie die Befehlszeile:

1. Öffnen Sie ein Eingabeaufforderungsfenster.

Wählen Sie **START > AUSFÜHREN >**, und geben Sie Folgendes ein: `cmd`

2. Navigieren Sie zum Endpoint Connect-Verzeichnis:

`C:\Program Files\CheckPoint\TRAC`

3. Geben Sie `command_line <Befehl> [<args>]` ein:

Dabei kann `<Befehl>` Folgendes sein:

Table 0-3 Befehlszeilenoptionen für Endpoint Connect

Befehl	Funktion
Start	Startet den Endpoint Connect-Service.
Stop	Stoppt den Endpoint Connect-Service.
Status	Gibt Statusinformationen aus und listet aktuelle Verbindungen auf.
info [-s <Sitename>]	Listet alle Verbindungen auf oder gibt Informationen zu Site-Namen aus.
connect [-s <Sitename>] [-u <Benutzername> -p <Kennwort> -d <dn> -f <p12> -pin <PIN> -sn <Seriennummer>]	Stellt anhand der vorhandenen Verbindung eine Verbindung her. • Der Parameter <Sitename> ist optional. Wird keine Site definiert, stellt der Client eine Verbindung mit der aktiven Site her. Ist keine aktive Site definiert, wird eine Fehlermeldung angezeigt. • Anmeldeinformationen können optional angegeben werden.
disconnect	Trennt die aktuelle Verbindung.
create -s <Sitename> [-a <Authentifizierungsverfahren>]	Erstellt eine neue Site und definiert ein Authentifizierungsverfahren. Gültige Authentifizierungswerte sind: • Benutzername-Kennwort • Zertifikat • p12-Zertifikat • Challenge Response • securIDKeyFob • securIDPinPad • SoftID Ein Administrator kann ein bestimmtes Authentifizierungsverfahren festlegen.

Befehl	Funktion
Start	Startet den Endpoint Connect-Service.
	Wird das falsche Verfahren verwendet, werden Sie aufgefordert, eine Alternative einzugeben.
delete -s <Sitename>	Löscht die vorhandene Verbindung.
help / h	Zeigt Informationen zum Verwenden des Befehls an.
list	Listet die im CAPI-Speicher vorhandenen Domännennamen auf.
ver	Zeigt die Endpoint Connect-Version an.
log	Zeigt Protokollmeldungen an.
enroll_p12 -s <Sitename> -f <Dateiname> -p <Kennwort> -r <Registrierungsschlüssel> [-l <Schlüssellänge>]	Registriert ein p12-Zertifikat.
renew_p12 -s <Sitename> -f <Dateiname> -p <Kennwort> [-l <Schlüssellänge>]	Erneuert ein p12-Zertifikat.
enroll_capi -s <Sitename> -r <Registrierungsschlüssel> [-i <Providerindex> -l <Schlüssellänge> -sp <hoheSchlüsselsicherheit>]	Registriert ein CAPI-Zertifikat.
renew_capi -s <Sitename> -d <dn> [-l <Schlüssellänge> -sp <hoheSchlüsselsicherheit>]	Erneuert ein CAPI-Zertifikat.
change_p12_pwd -f <Dateiname> [-o <altesKennwort> -n <neues Kennwort>]	Ändert das p12-Kennwort

Antivirus und Anti-Spyware

Die integrierten, leistungsstarken Antivirus- und Anti-Spyware-Funktionen schützen Ihren Computer sowohl vor Viren als auch vor Spyware. Verschiedene Prüfungsoptionen erkennen Viren und Spyware automatisch und machen sie unschädlich, bevor Schäden auf Ihrem Computer entstehen.

Inhalt dieses Abschnitts

Endpoint Security Antivirus und Anti-Spyware	57
Prüfen	59
Erweiterte Optionen	65

Endpoint Security Antivirus und Anti-Spyware

Die Antivirus schützt Ihren Computer vor bekannten und unbekannten Viren. Dabei werden Dateien überprüft, mit einer Datenbank bekannter Viren verglichen und auf bestimmte virentypische Merkmale untersucht. Dateien können geprüft werden, wenn Sie geöffnet oder geschlossen sind, während sie ausgeführt werden oder als Teil einer Prüfung des gesamten Computers. Wird ein Virus gefunden, macht Endpoint Security ihn unschädlich, indem die Datei repariert oder der Zugriff auf die Datei verweigert wird.

Die Anti-Spyware-Funktion erkennt Spyware-Komponenten auf Ihrem Computer und entfernt sie automatisch oder stellt sie unter Quarantäne, so dass Sie sie manuell entfernen können, nachdem Sie das von ihnen ausgehende Risiko eingeschätzt haben.

Antivirus und Anti-Spyware aktivieren

Bevor Sie die Antivirus-Schutzfunktion aktivieren, müssen Sie alle anderen Antivirus-Programme von Ihrem Computer löschen, auch Suite-Produkte, die

Virenschutzprogramme enthalten. Der Endpoint Security Client kann einige Antivirus-Anwendungen automatisch für Sie deinstallieren. Wenn Sie ein Programm verwenden, das nicht automatisch deinstalliert werden kann, verwenden Sie die Option **Software** der Windows-Systemsteuerung.

So aktivieren Sie den Viren- und Spyware-Schutz:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie im Bereich Antivirus auf Ein.
3. Klicken Sie im Bereich Anti-Spyware auf Ein.

Anzeigen des Viren- und Spyware-Schutzstatus

Um den Status Ihres Virus- und Spyware-Schutzes anzuzeigen, öffnen Sie **Überblick | Grundeinstellungen** oder **Antivirus/spyware | Grundeinstellungen**.

Auf der Registerkarte des Bildschirms Antivirus / Anti-Spyware wird der Status Ihres Viren- und Spyware-Schutzes angezeigt. In diesem Bereich können Sie Folgendes tun:

- Sicher stellen, dass der Viren- und Spyware-Schutz aktiviert ist
- Datum und Uhrzeit Ihrer letzten Prüfungen einsehen
- Definitionsdateien aktualisieren
- Eine Prüfung starten
- Die Ergebnisse der letzten Prüfung anzeigen
- Auf erweiterte Einstellungen zugreifen

Weitere Informationen zu den Statusinformationen auf dem Bildschirm finden Sie unter **Verwendung der Registerkarte Status** siehe "[Verwenden der Registerkarte „Grundeinstellungen“ von „Überblick“](#)" auf Seite 15.

Aktualisieren von Antivirus und Anti-Spyware

Alle Antiviren- oder Anti-Spyware-Anwendungen enthalten eine Definitionsdatei mit Informationen, die das Identifizieren und Lokalisieren von Viren und Spyware auf dem Computer ermöglichen. Wenn neue Viren oder Spyware-Anwendungen gefunden werden, aktualisiert der Client seine Datenbank mit den Definitionsdateien, die zur Erkennung dieser neuen Bedrohungen erforderlich sind.

Der Computer ist folglich anfällig für Viren und Spyware, wenn die Datenbank der Virendefinitionsdateien veraltet ist.

Unter Antivirus/Spyware | Grundeinstellungen können Sie feststellen, ob Antivirus oder Anti-Spyware aktualisiert werden müssen.

So erhalten Sie Aktualisierungen auf Anfrage:

1. Öffnen Sie Antivirus/Spyware | Grundeinstellungen.
2. Klicken Sie auf **Jetzt aktualisieren**, falls im Antivirus- oder Anti-Spyware-Bereich **Aktualisierung überfällig** angezeigt wird.

Prüfen

Es gibt mehrere Möglichkeiten, eine Prüfung auf Ihrem Computer zu starten.

- Klicken Sie auf der Registerkarte **Antivirus-spyware | Grundeinstellungen** auf **Auf Viren prüfen**, **Auf Spyware prüfen** oder **Auf Viren/Spyware prüfen**.
- Klicken Sie mit der rechten Maustaste auf eine Datei auf Ihrem Computer, und wählen Sie **Prüfen mit Check Point Antivirus** aus.
- Planen Sie eine Systemprüfung, die einmal oder in regelmäßigen Abständen ausgeführt wird.
- Öffnen Sie eine Datei (wenn die Prüfung bei Zugriff aktiviert ist).

Sie können bis zu fünf Prüfungen gleichzeitig durchführen. Die Prüfungen werden in der Reihenfolge durchgeführt, in der Sie gestartet wurden.

Systemprüfungen bieten zusätzlichen Schutz, indem sie Ihnen ermöglichen, alle Inhalte Ihres Computers auf einmal zu prüfen. Systemprüfungen finden inaktive Viren, die sich auf der Festplatte Ihres Computers befinden. Wenn Sie regelmäßig Systemprüfungen durchführen, können Sie sicherstellen, dass Ihre Antivirus-Signaturdateien immer auf dem neuesten Stand sind.

Da Systemprüfungen sehr gründlich sind, können sie einige Zeit in Anspruch nehmen. Aus diesem Grund beeinträchtigen vollständige Systemprüfungen unter Umständen die Leistung Ihres Systems. Damit Ihre Abläufe nicht behindert werden, können Sie Systemprüfungen für Zeiten planen, zu denen Sie voraussichtlich nicht an Ihrem Computer arbeiten.



Hinweis - Wenn Sie im Dialogfeld **Prüfung** während einer Prüfung auf **Pause** klicken, wird lediglich die aktuelle Prüfung angehalten. Die Prüfung bei Zugriff wird nicht deaktiviert. Wenn Sie erneut auf **Pause** klicken, wird die aktuelle Prüfung fortgesetzt.

Während der Prüfung ist die Schaltfläche **Erweiterte Optionen**

deaktiviert.

Grundlegendes zu Prüfungsergebnissen

Die Ergebnisse der Prüfung werden im Fenster Prüfungsergebnisse angezeigt.

Table 0-4 Informationen in Prüfungsergebnisse

Name	Name des Virus/der Spyware.
Behandlung	Gibt die für die Infektion/Spyware verwendete Behandlung an: In Quarantäne oder Gelöscht.
Risiko	Zeigt die Risikostufe der Infektion an. • Hoch: Bedrohung für die Sicherheit. Bei allen Viren wird ein hohes Risiko angenommen. • Mittel: Potenzielle Verletzung der Privatsphäre. • Niedrig: Adware oder andere unschädliche, jedoch lästige Software.
Pfad	Speicherort des Virus/der Spyware.
Typ	Gibt an, ob die Infektion von einem Virus, Wurm oder Trojaner verursacht wurde oder ob es sich bei der Spyware um Keylogging-Software oder einen Tracking-Cookie handelt. Status: Gibt darüber Aufschluss, ob die Datei repariert bzw. gelöscht wurde oder noch infiziert ist. Wenn der Client das Element nicht behandeln konnte, wird hier möglicherweise ein Link mit der Weiteren Vorgehensweise angezeigt. Über diesen Link gelangen Sie zu weiteren Informationen und Anweisungen. Informationen: Liefert weitere Einzelheiten. Um weitere Informationen zu einem Virus oder zu einer Spyware zu erhalten, klicken Sie auf den Link Weitere Informationen .
Detail	Aktive Elemente: Infektionen/Spyware-Programme, die während der Prüfung gefunden wurden und nicht automatisch behandelt werden konnten. Um die empfohlenen Behandlungsmethoden in der Spalte Behandlung anzunehmen, klicken Sie auf Übernehmen . Autom. Behandlung: Bereits behandelte Elemente. Sie müssen keine weiteren Maßnahmen ergreifen.

Manuelle Behandlung von Dateien

Wenn Sie die automatische Behandlung nicht aktiviert haben oder eine Datei nicht automatisch repariert werden konnte, können Sie sie über das Fenster mit den Details der Prüfung manuell behandeln.

So behandeln Sie eine Datei manuell:

1. Wählen Sie im Fenster **Prüfungsergebnisse** das zu behandelnde Element aus.
2. Wählen Sie in der Spalte **Behandlung** die gewünschte Behandlungsoption aus
3. Klicken Sie auf **Schließen**, wenn Sie mit der Behandlung der Datei fertig sind.

Table 0-5 Optionen für die Virenprüfung

Reparieren	Versucht, die ausgewählte Datei zu reparieren.
Quarantäne	Hängt die Erweiterung .zl6 an die infizierte Datei an, um sie unschädlich zu machen. Die Datei wird unter Quarantäne gestellt.
Umbenennen	Ermöglicht Ihnen, die Datei umzubenennen, so dass sie bei zukünftigen Prüfungen nicht mehr gefunden wird. Verwenden Sie diese Option nur dann, wenn Sie sich ganz sicher sind, dass die Datei kein Virus ist.
Löschen	Löscht die ausgewählte Datei.
Beim Neustart löschen	Löscht die ausgewählte Datei, wenn Ihr Computer das nächste Mal neu gestartet wird.
Immer ignorieren	Weist den Client an, die Datei bei allen zukünftigen Prüfungen zu ignorieren.
Einmal ignorieren	Weist den Client an, das Element aus der Liste zu entfernen und keine weiteren Maßnahmen zu ergreifen.

Wenn die Ergebnisse einer Prüfung die Meldung **Fehler, Keine Behandlung verfügbar** oder **Behandlung fehlgeschlagen** enthalten, gibt es derzeit keine sichere Möglichkeit zur automatischen Entfernung des Virus, ohne die Integrität des Computers oder anderer Dateien zu gefährden.

Um manuelle Behandlungsmöglichkeiten in Erfahrung zu bringen, geben Sie den Namen des Virus zusammen mit dem Wort „Removal“ oder „Entfernen“ in eine Suchmaschine wie Google oder Yahoo ein und suchen auf diese Weise nach Anweisungen zum Entfernen.

Check Point sucht permanent nach Viren und entwickelt sichere Methoden für deren Entfernung.

Senden von Viren und Spyware an Check Point

Wenn Sie potenzielle Malware an Check Point weiterleiten, unterstützen Sie uns dabei, die Sicherheit und den Schutz aller Internetnutzer zu erhöhen. Das Sicherheitsteam von Check Point überprüft alle eingehenden Einsendungen auf neue Dateien. Das Sicherheitsteam von Check Point reagiert gegebenenfalls auf

Ihre Einsendung und wird Sie möglicherweise kontaktieren, um weitere Informationen oder Einzelheiten zu den von Ihnen gesendeten Dateien zu erhalten.

Auf Grund des Umfangs der täglich veröffentlichten Malware können unsere Mitarbeiter nicht jede Ihrer Einsendungen beantworten. Dennoch wissen wir Ihre Hilfe zu schätzen und möchten Ihnen danken, dass Sie sich die Zeit nehmen, um uns dabei zu unterstützen, das Internet sicherer zu machen. Richten Sie alle Fragen oder Anmerkungen an: security@checkpoint.com

So senden Sie Malware zur Überprüfung an Check Point:

1. Speichern Sie die Malware in einem kennwortgeschützten ZIP-Archiv, und legen Sie als Kennwort *infected* (infiziert) fest.

Wie Sie ein kennwortgeschütztes Archiv erstellen, erfahren Sie in der Hilfe zu WinZip.

2. Senden Sie die ZIP-Datei an malware@checkpoint.com

Verwenden Sie diese E-Mail-Adresse nur, wenn Sie Malware an das Sicherheitsteam von Check Point senden.



Wichtig - Senden Sie keine Dateien mit Malware, wenn Sie befürchten, dass der Vorgang nicht sicher ist, oder dadurch das Risiko einer Infektion oder Beschädigung Ihres Systems erhöht wird. Senden Sie keine Dateien mit potenzieller Malware an andere, da sie schädlich sein können.

Anzeigen von Elementen in Quarantäne

In einigen Fällen können Elemente, die während einer Viren- oder Spyware-Prüfung gefunden wurden, nicht automatisch behandelt werden. Diese Elemente werden in der Regel unter Quarantäne gestellt, so dass sie zwar unschädlich gemacht werden, jedoch erhalten bleiben und später behandelt werden können, nachdem die Viren- oder Spyware-Signaturdateien aktualisiert wurden.

So zeigen Sie Spyware in Quarantäne an:

1. Öffnen Sie Antivirus/spyware.
2. Öffnen Sie die Registerkarte Quarantäne.
3. Wählen Sie Viren oder Spyware in der Dropdown-Liste In Quarantäne aus.

Table 0-6 Quarantäneinformationen für Viren

Infektion	Der Name des Virus.
-----------	---------------------

Tage unter Quarantäne	Die Anzahl der Tage, die die Datei in Quarantäne ist.
Pfad	Der Speicherort des Virus auf Ihrem Computer.
Table 0-7 Quarantäneinformationen für Spyware	
Typ	Art der Spyware: Keylogging oder Cookie.
Name	Der Name der Spyware.
Risiko	Die Risikostufe der Infektion: ob sie niedrig ist, wie bei Adware, oder eine ernsthafte Bedrohung darstellt, wie bei Keylogging-Software.
Tage unter Quarantäne	Die Anzahl der Tage, die die Datei in Quarantäne ist.

Behandeln von Elementen in Quarantäne

Sie können Viren oder Spyware unter Quarantäne stellen oder die Quarantäne aufheben.

So löschen Sie ein unter Quarantäne stehendes Element bzw. stellen dieses wieder her:

1. Öffnen Sie Antivirus/spyware! Grundeinstellungen.
2. Wählen Sie Spyware oder Viren in der Dropdown-Liste In Quarantäne aus.
3. Wählen Sie das Element in der Liste aus.
 - Klicken Sie auf Löschen, um das Element in den Papierkorb zu verschieben.
 - Klicken Sie auf Wiederherstellen, um das Element an seinen ursprünglichen Speicherort zu transferieren. Verwenden Sie diese Option mit Vorsicht, wenn Sie keine Dateien wiederherstellen wollen, die schädlich sein können.
 - Um ein Element zur Analyse an Check Point zu senden, wählen Sie das Element aus und klicken Sie auf Mehr Info.

Anzeigen von Protokollen

Standardmäßig werden alle Viren- und Spyware-Ereignisse in der Protokollanzeige festgehalten.

So zeigen Sie protokollierte Virenereignisse an:

1. Öffnen Sie Warnungen & Protokolle | Protokollanzeige.
2. Wählen Sie in der Dropdown-Liste Warnmeldungstyp Antivirus oder Anti-Spyware aus.

Table 0-8 Protokollinformationen

Feld	Informationen
Datum	Das Datum der Infektion.
Typ	Der Typ des aufgetretenen Ereignisses: Viren Spyware • Aktualisierung • Prüfung • Behandlung • E-Mail • Adware • Objekt für Browserhilfe • Dialer • Keylogger • Spy-Cookie
Virusname/Spyware-Name	Der gängige Name des Virus (beispielsweise <i>iloveyou.exe</i>) oder der Spyware (beispielsweise <i>NavExcel</i>).
Dateiname	Der Name der infizierten Datei, der Name der geprüften Dateien oder der Name und die Versionsnummer der Aktualisierung und/oder der Engine.
Maßnahme	Vom Client durchgeführte Behandlung des Virus: • Aktualisiert, Aktualisierung abgebrochen, Aktualisierung fehlgeschlagen • Geprüft, Prüfung abgebrochen, Prüfung fehlgeschlagen • Datei repariert, Dateireparatur fehlgeschlagen • In Quarantäne, Quarantäne fehlgeschlagen • Gelöscht, Löschen fehlgeschlagen • Wiederhergestellt, Wiederherstellung fehlgeschlagen • Umbenannt, Umbenennen fehlgeschlagen
Akteur	Gibt an, ob die Maßnahme manuell oder

Feld	Informationen
	automatisch durchgeführt wurde.
E-Mail	Wenn der Virus in einer E-Mail gefunden wurde, die E-Mail-Adresse des Absenders.

Erweiterte Optionen

Die Schaltfläche **Erweiterte Optionen** ist aktiviert, wenn die persönliche Richtlinie (siehe **Richtlinien**) die einzige aktive Richtlinie ist.

Falls eine Unternehmensrichtlinie oder getrennte Richtlinie aktiv ist, werden die Funktionen dieser Option vom SystemAdministrator gesteuert.

Aus diesem Grund können Sie die erweiterten Optionen Ihres eigenen Clients nur dann steuern, wenn die UnternehmensRichtlinie noch nicht empfangen wurde und keine Verbindung zum Endpoint Security Server besteht oder die zugewiesene Richtlinie nur aus einer UnternehmensRichtlinie besteht und Ihr Client vom Server getrennt ist.

Planen von Prüfungen

Ihren Computer auf Viren und Spyware zu prüfen, ist eine der wichtigsten Maßnahmen, die Sie ergreifen können, um die Integrität Ihren Daten und Ihrer EDV-Umgebung zu schützen. Prüfungen sind am effektivsten, wenn sie regelmäßig ausgeführt werden. Daher ist es sinnvoll, die Prüfung als Aufgabe zu planen, die automatisch ausgeführt wird. Ist Ihr Computer zum Zeitpunkt einer geplanten Prüfung nicht eingeschaltet, wird die Prüfung 15Minuten nach dem Start des Computers durchgeführt.

So planen Sie eine Prüfung:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Im Bereich Antivirus auf den Link **Zum Planen** klicken.
Das Fenster **Erweiterte Optionen** wird angezeigt.
3. Aktivieren Sie unter den Optionen von **Prüfung planen** das Kontrollkästchen **Auf Viren prüfen**, und geben Sie dann einen Tag und eine Uhrzeit für die Prüfung an.
4. Geben Sie das Prüfungsintervall an: täglich, wöchentlich oder monatlich.

5. Aktivieren Sie das Kontrollkästchen **Auf Spyware prüfen**, und geben Sie dann einen Tag und eine Uhrzeit für die Prüfung an.
6. Geben Sie das Prüfungsintervall an.
7. Klicken Sie auf **OK**.



Hinweis - Wenn Sie eine wöchentliche Prüfung planen, wird die Prüfung an dem Wochentag des Startdatums ausgeführt. Wurde das Startdatum beispielsweise auf den 4. November 2008 festgelegt, erfolgt die Prüfung an jedem nachfolgenden Dienstag.

Aktualisieren von Viren- und Spyware-Definitionen

Alle Antiviren- oder Anti-Spyware-Anwendungen enthalten eine Definitionsdatei mit Informationen, die das Identifizieren und Lokalisieren von Viren und Spyware auf Ihrem Computer ermöglichen. Wenn neue Viren oder Spyware-Anwendungen gefunden werden, aktualisiert der Client seine Datenbank mit den Definitionsdateien, die zur Erkennung dieser neuen Bedrohungen erforderlich sind. Ihr Computer ist folglich anfällig für Viren und Spyware, wenn die Datenbank der Virendefinitionsdateien veraltet ist.

Wenn Sie die Funktion zur automatischen Aktualisierung aktivieren, erhalten Sie immer die aktuellsten Definitionsdateien, sobald sie verfügbar sind.

So aktivieren Sie automatische Aktualisierungen:

1. Öffnen Sie **Antivirus/spyware | Grundeinstellungen**.
2. Klicken Sie auf **Erweiterte Optionen**.
Das Fenster **Erweiterte Optionen** wird angezeigt.
3. Zeigen Sie die Optionen von **Aktualisierungen** an.
4. Aktivieren Sie das Kontrollkästchen **Automatische Antivirus-Aktualisierungen aktivieren**.
5. Aktivieren Sie das Kontrollkästchen **Automatische Anti-Spyware-Aktualisierungen aktivieren**.
6. Legen Sie in der Dropdown-Liste **Aktualisierungshäufigkeit einstellen** fest, wann der Client auf Aktualisierungen prüfen und diese bei Verfügbarkeit herunterladen und installieren soll.
7. Klicken Sie auf **OK**.

Auf Antivirus/spyware | Grundeinstellungen können Sie feststellen, ob Antivirus oder Anti-Spyware aktualisiert werden muss.

So erhalten Sie Aktualisierungen auf Anfrage:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Falls Aktualisierung überfällig im Antivirus oder Anti-Spyware-Bereich angezeigt wird, klicken Sie auf den Link Zum Aktualisieren klicken, oder klicken Sie auf Jetzt aktualisieren.

Festlegen von Zielen für die Prüfung

Sie können festlegen, welche Laufwerke, Ordner und Dateien bei einer Systemprüfung geprüft werden sollen. Sie können ein Element in die Prüfung einschließen oder davon ausschließen, indem Sie auf das Kontrollkästchen neben dem jeweiligen Element klicken. Standardmäßig prüft der Client nur lokale Festplatten.

So geben Sie Ziele für die Prüfung an:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
Das Fenster Erweiterte Optionen wird angezeigt.
3. Öffnen Sie Virus-Verwaltung| Ziele prüfen.
4. Geben Sie an, welche Laufwerke, Ordner und Dateien geprüft werden sollen.
5. Aktivieren Sie das Kontrollkästchen Boot-Sektoren aller lokalen Laufwerke prüfen, und klicken Sie dann auf OK.
6. Aktivieren Sie das Kontrollkästchen Systemspeicher prüfen, und klicken Sie dann auf OK.

In der folgenden Tabelle werden die Symbole aus dem Fenster Ziele prüfen erklärt.

Table 0-9 Symbole, die Ziele für die Prüfung kennzeichnen

Symbol	Beschreibung
	Die ausgewählte Festplatte und alle Unterordner und Dateien werden in die Prüfung einbezogen.
	Die ausgewählte Festplatte und alle Unterordner und Dateien werden von der Prüfung ausgeschlossen.
	Die ausgewählte Festplatte wird in die Prüfung einbezogen, jedoch wird mindestens ein Unterordner oder eine Datei von der Prüfung ausgeschlossen.
	Der ausgewählte Ordner wird von der Prüfung ausgeschlossen, jedoch wird mindestens ein Unterordner oder eine Datei in die Prüfung einbezogen.
 	Der ausgewählte Ordner wird in die Prüfung einbezogen. Ein graues Häkchen bedeutet, dass die Prüfung des Ordners oder der Datei aktiviert ist, da die Prüfung für eine übergeordnete Festplatte oder einen übergeordneten Ordner aktiviert wurde.
 	Der ausgewählte Ordner wird von der Prüfung ausgeschlossen. Ein graues x bedeutet, dass die Prüfung des Ordners oder der Datei deaktiviert ist, da die Prüfung für eine übergeordnete Festplatte oder einen übergeordneten Ordner deaktiviert wurde.
Andere	RAM-Laufwerke und alle unbekannten Laufwerke. Geben Sie an, welche anderen Laufwerke geprüft werden sollen.

Prüfen bei Zugriff

Durch Prüfen bei Zugriff wird Ihr Computer geschützt, indem inaktive Viren, die sich möglicherweise auf Ihrem Computer befinden, gefunden und unschädlich gemacht werden. Prüfen bei Zugriff ist standardmäßig aktiviert und bietet die aktivste Form des Virenschutzes. Dateien werden auf Viren geprüft, sobald sie geöffnet, ausgeführt oder geschlossen werden. Auf diese Weise können Viren sofort gefunden und unschädlich gemacht werden.



Hinweis - Prüfen bei Zugriff prüft ein Archiv (komprimierte Datei, beispielsweise mit der Erweiterung* .zip) nur dann auf Viren, wenn die Datei geöffnet wird. Im Gegensatz zu anderen Dateitypen werden Archive nicht geprüft, wenn Sie diese von einem Speicherort zu einem anderen verschieben.

Prüfen bei Zugriff unterstützt keine anderen Antivirus-Provider und wird deaktiviert, wenn Sie keine Check Point Antivirus nutzen.

So aktivieren Sie die Option „Prüfen bei Zugriff“:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
3. Öffnen Sie Virus-Verwaltung| Prüfen bei Zugriff, und aktivieren Sie dann das Kontrollkästchen Prüfen bei Zugriff aktivieren.
4. Klicken Sie auf OK.

Angeben von Spyware-Erkennungsmethoden

Zusätzlich zur standardmäßigen Erkennung, die die Registrierung Ihres Computers nach aktiver Spyware durchsucht, gibt es Methoden für die Erkennung von ruhender und schwer zu findender Spyware.

So legen Sie Spyware-Erkennungsmethoden fest:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
3. Öffnen Sie Spyware-Verwaltung| Erkennung.
4. Aktivieren Sie das Kontrollkästchen Nach Cookies suchen.
5. Legen Sie unter Erkennungsoptionen mit maximaler Stärke fest, ob die Prüfung umfassender oder schneller sein soll:
 - Intelligente Schnellprüfung: Standardmäßig aktiviert.
 - Ganzes System prüfen: Prüft das lokale Dateisystem.
 - Tiefen-Prüfung: Prüft jedes Datenbyte auf Ihrem Computer.

Die Optionen Ganzes System prüfen und Tiefen-Prüfung können die Systemleistung beeinträchtigen. Wählen Sie eine dieser Optionen nur dann aus, wenn der Verdacht besteht, dass unerkannte Spyware vorliegt.

6. Klicken Sie auf OK.

Aktivieren der automatischen Virenbehandlung

Wenn eine Vireninfektion gefunden wurde, werden im Fenster Prüfung die verfügbaren Behandlungsoptionen wie Quarantäne, Reparieren oder Löschen angezeigt. Der Client versucht standardmäßig, Dateien, die Viren enthalten, automatisch zu behandeln. Lässt sich eine Datei nicht reparieren, werden Sie im

Fenster **Prüfung** darüber informiert, so dass Sie entsprechende Maßnahmen ergreifen können.

So aktivieren Sie die automatische Virenbehandlung:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
3. Öffnen Sie Virus-Verwaltung | Automatische Behandlung.
4. Wählen Sie die gewünschte Option für die automatische Behandlung aus:
 - Warnen - nicht automatisch behandeln
 - Versuchen zu reparieren, warnen, wenn Reparatur fehlschlägt
 - Versuchen zu reparieren, unter Quarantäne stellen, wenn Reparatur fehlschlägt (empfohlen)
5. Klicken Sie auf OK.

Aktivieren der automatischen Spyware-Behandlung

Wenn Spyware gefunden wurde, werden im Fenster **Prüfung** die verfügbaren Behandlungsoptionen wie **Quarantäne** oder **Löschen** angezeigt. Die empfohlene Spyware-Behandlung wird im Fenster **Prüfung** vorgeschlagen, so dass Sie die erforderlichen Maßnahmen ergreifen können.

So aktivieren Sie die automatische Spyware-Behandlung:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
3. Öffnen Sie Spyware-Verwaltung | Automatische Behandlung.
4. Aktivieren Sie das Kontrollkästchen **Automatische Spyware-Behandlung aktivieren**, und klicken Sie anschließend auf OK.

Reparieren von Dateien in einem Archiv

Wenn sich die infizierte Datei in einer Archivdatei befindet (z. B. einer ZIP-Datei), kann der Client sie nicht behandeln.

So reparieren Sie eine Datei in einem Archiv:

1. Stellen Sie sicher, dass Prüfung bei Zugriff aktiviert ist.
2. Öffnen Sie die im Fenster **Prüfungsergebnisse** aufgeführte Datei über ein Archivierungsdienstprogramm, beispielsweise WinZip.

Die Prüfung bei Zugriff prüft die Datei auf Infektionen. Die Ergebnisse der Prüfung werden anschließend im Fenster **Prüfungsergebnisse** angezeigt.
3. Extrahieren Sie die Dateien von dem zu behandelnden Archiv, und starten Sie die Prüfung erneut.

Optionen für die Virenprüfung

Sie können Ihre Virenprüfung so konfigurieren, dass alle Dateien, die eine bestimmte Größe (Standardeinstellung ist 8 MB) überschreiten, ignoriert werden. Durch diese Option, wird die Prüfzeit ohne erhöhtes Risiko verkürzt, da Virendateien normalerweise kleiner als 8 MB sind. Auch wenn große Dateien, die von der Prüfung ignoriert werden, möglicherweise Viren enthalten, ist Ihr Computer weiterhin geschützt, wenn Sie **Prüfen bei Zugriff** aktiviert haben.

Sie können auch die erweiterte Datenbank aktivieren. Diese Datenbank enthält zusätzlich zu der Standardvirenliste eine umfassende Liste mit Malware. Allerdings kann sich manche in der Liste aufgeführte Malware auch in der standardmäßigen Anti-Spyware-Datenbank befinden, so dass die eine oder andere potenzielle Malware doppelt geprüft wird. Auch die Malware-Liste der erweiterten Datenbank kann Programme enthalten, die als nützlich gelten.

So legen Sie Optionen für die Virenprüfung fest:

1. Öffnen Sie Antivirus/spyware! Grundeinstellungen.
2. Klicken Sie auf **Erweiterte Optionen**.

Das Fenster **Erweiterte Optionen** wird angezeigt.
3. Öffnen Sie **Virus-Verwaltung! Prüfungsoptionen**.
4. Aktivieren Sie das Kontrollkästchen **Überspringen**, wenn das Objekt größer ist als, und geben Sie eine maximale Objektgröße in das Feld MB ein.
5. Wählen Sie in der Dropdown-Liste **Prüfungspriorität festlegen** eine Option aus:
 - Hoch (Schnelle Prüfungen, PC langsamer)
 - Mittel

- Niedrig (Langsame Prüfungen, PC schneller)
6. Klicken Sie auf OK.

Antivirus-Ausnahmenliste

Obwohl einige Programme, die von der erweiterten Datenbank als verdächtig eingestuft werden, Ihren Computer möglicherweise beschädigen oder Ihre Daten Hackerangriffen aussetzen können, gibt es auch viele nützliche Anwendungen, die bei einer Prüfung ebenfalls als Viren erkannt werden. Wenn Sie eine dieser Anwendungen verwenden, können Sie sie von den Antivirus-Prüfungen ausschließen, indem Sie sie der Ausnahmenliste hinzufügen.

So fügen Sie der Ausnahmenliste Programme hinzu:

- Klicken Sie in der Liste Prüfungsergebnisse auf das Programm, und wählen Sie Immer ignorieren aus. Oder:
 1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
 2. Klicken Sie auf Erweiterte Optionen.
 3. Öffnen Sie Virus-Verwaltung|Ausnahmen.
 4. Klicken Sie im Bereich Virenbehandlung - Ausnahmen auf Datei hinzufügen.
Das Fenster Ausnahme hinzufügen wird geöffnet. Es enthält Beispiele für Ausnahmen, die hinzugefügt werden können.
 5. Geben Sie eine Ausnahme wie in den Beispielen an, oder klicken Sie auf Durchsuchen, und wählen Sie die Datei, den Ordner oder das Laufwerk für den Ausschluss von der Prüfung aus.
 6. Klicken Sie auf OK.

Falls Sie einen Virus versehentlich der Ausnahmenliste hinzugefügt haben, können Sie ihn wieder entfernen.

So entfernen Sie Viren von der Ausnahmenliste:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
3. Öffnen Sie Virus-Verwaltung|Ausnahmen.
4. Wählen Sie im Bereich Virenbehandlung - Ausnahmen den Virus aus, den Sie entfernen möchten, und klicken Sie dann auf Von Liste entfernen.

5. Klicken Sie auf OK.

Anti-Spyware Ausnahmeliste

Obwohl einige Spyware-Programme möglicherweise Ihren Computer oder Ihre Daten beschädigen, gibt es auch viele harmlose Anwendungen, die bei einer Prüfung als Spyware erkannt werden könnten. Wenn Sie eine dieser Anwendungen verwenden (beispielsweise Spracherkennungs-Software), können Sie sie von den Spyware-Prüfungen ausschließen, indem Sie sie der Ausnahmeliste hinzufügen.

So fügen Sie der Ausnahmeliste Programme hinzu:

- Klicken Sie in der Liste Prüfungsergebnisse mit der rechten Maustaste auf das Programm, und wählen Sie Immer ignorieren aus.

Falls Sie ein Spyware-Programm versehentlich der Ausnahmeliste hinzugefügt haben, können Sie es wieder entfernen.

So entfernen Sie Spyware aus der Ausnahmeliste:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie auf Erweiterte Optionen.
3. Öffnen Sie Spyware-Verwaltung|Ausnahmen.
4. Wählen Sie im Bereich Spyware-Behandlung - Ausnahmen die Spyware-Anwendung aus, die Sie entfernen möchten, und klicken Sie dann auf Von Liste entfernen.
5. Klicken Sie auf OK.

Firewall

Firewallschutz ist Ihre beste Verteidigungsstrategie gegen Bedrohungen aus dem Internet. Die Standardzonen und Sicherheitsstufen des Clients schützen Sie sofort nach der Installation vor praktisch allen Bedrohungen aus dem Internet.

Inhalt dieses Abschnitts

Firewall-Schutz verstehen	75
Grundlegendes zu Zonen	76
Konfigurieren neuer Netzwerkverbindungen	78
Integrieren in Netzwerkdienste	78
Auswählen der Sicherheitsstufen	80
Festlegen von erweiterten Sicherheitsoptionen	81
Verwalten von Zonendatenverkehr	85
Sperren und Freigeben von Ports	89
Konfigurieren der VPN-Verbindung für Firewall	92

Firewall-Schutz verstehen

In Gebäuden wird die Ausbreitung von Bränden durch eine Firewall (Brandschutzwand) verhindert. Dieser Ausdruck hat Eingang in die Computerwelt gefunden. Im Internet können gefährliche Brände auf verschiedene Art und Weise verursacht werden, z. B. durch Hackerangriffe, Viren oder Würmer. Eine Firewall ist ein System, das Angriffsversuche, die Ihren Computer beschädigen könnten, verhindert.

Die Firewall des Clients bewacht die „Türen“ zu Ihrem Computer, also die Ports, die der eingehende und ausgehende Internet-Datenverkehr passiert. Der Client untersucht den gesamten Netzwerkverkehr, der bei Ihrem Computer eingeht, und stellt folgende Fragen:

- Aus welcher Zone stammt der Datenverkehr, und an welchen Port ist er adressiert?
- Erlauben die Einstellungen für die Zone den Datenverkehr über diesen Port?
- Verstößt der Datenverkehr gegen irgendwelche globale Regeln?
- Hat der Datenverkehr von einem Programm auf Ihrem Computer die nötige Berechtigung erhalten (Einstellungen für Program Control)?

Mit Hilfe der Antworten auf diese Fragen wird bestimmt, ob der Datenverkehr zugelassen oder gesperrt wird.

Grundlegendes zu Zonen

Der Endpoint Security verfolgt alle harmlosen, böswilligen und unbekannten Internetaktivitäten mit Hilfe von virtuellen Behältern, so genannten *Zones*, mit denen Computer und Netzwerke, die mit Ihrem Computer verbunden sind, klassifiziert werden.

Die **Internetzone** auf Seite [201](#) ist die „unbekannte Zone“. Alle Computer und Netzwerke zählen zu dieser Zone, bis sie von Ihnen einer anderen Zone zugeordnet werden.

Die **Sichere Zone** auf Seite [207](#) wird als „harmlos“ eingestuft. Sie umfasst alle Computer und Netzwerke, denen Sie vertrauen und mit denen Sie Ressourcen austauschen möchten (z.B. die anderen Computer in Ihrem lokalen Netzwerk/Heimnetzwerk).

Die **Gesperrte Zone** auf Seite [200](#) wird als „böswillig“ eingestuft. Sie umfasst Computer und Netzwerke, denen Sie misstrauen.

Wenn ein anderer Computer mit Ihrem Rechner Daten austauschen will, überprüft der Client, in welcher Zone sich dieser Computer befindet, und entscheidet dann, ob der Datenaustausch zugelassen oder gesperrt werden soll.

Verwaltung der Firewall-Sicherheit nach Zonen

Der Client bestimmt an Hand von Sicherheitsstufen, ob eingehender Datenverkehr aus der jeweiligen Zone zugelassen oder gesperrt werden soll. Öffnen Sie im Bildschirm **Firewall** die Registerkarte **Grundeinstellungen**, um die Sicherheitsstufen anzeigen und anpassen.

Einstellung für hohe Sicherheit

Bei der Einstellung für hohe Sicherheit wird Ihr Computer in den Stealth-Modus versetzt, so dass er von Hackern nicht erkannt wird. Die Einstellung für hohe Sicherheit ist die Standardkonfiguration der Internetzone.

Bei der Einstellung für hohe Sicherheit sind die Datei- und Druckerfreigabe deaktiviert. Ausgehender DNS- und DHCP-Datenverkehr sowie Rundsendungen und Multicast sind jedoch zulässig, so dass Sie im Internet surfen können. Alle anderen Ports Ihres Computers sind geschlossen, sofern sie nicht von einem Programm mit Zugriffsrechten bzw. Serverberechtigungen verwendet werden.

Einstellung für mittlere Sicherheit

Die Einstellung für mittlere Sicherheit ist die Standardeinstellung für die Sichere Zone.

Bei der Einstellung für mittlere Sicherheit sind die Datei- und Druckerfreigabe aktiviert und alle Ports und Protokolle zugelassen. (In der Internetzone wird allerdings bei der Einstellung für mittlere Sicherheit eingehender NetBIOS-Datenverkehr gesperrt. Dies schützt Ihren Computer vor möglichen Angriffen auf die Windows-Netzwerkdienste.) Bei mittlerer Sicherheit befindet sich der Computer nicht mehr im Stealth-Modus.

Es wird empfohlen, nach der Installation des Clients während der ersten Tage bei regulärem Internetgebrauch die mittlere Sicherheitseinstellung zu verwenden. Nach einigen Tagen normalen Internetgebrauchs kennt der Client die Signaturen der meisten Komponenten, die Ihre Internetprogramme benötigen. Das Programm erinnert Sie dann daran, die Stufe für die Programmauthentifizierung auf Hoch einzustellen.

Für die Gesperrte Zone wird keine Sicherheitsstufe benötigt, da ein Datenaustausch mit dieser Zone nicht zulässig ist.



Hinweis - Erfahrene Benutzer können die Sicherheitseinstellungen Hoch und Mittel für jede Zone anpassen, indem sie einzelne Ports öffnen oder sperren. Siehe ***Sperren und Freigeben von Ports*** auf Seite [89](#).

Program Control über Zonen

Wenn ein Programm **Zugriffsrechte** siehe "[Zugriffsberechtigung](#)" auf Seite [209](#) oder eine **Serverberechtigung** auf Seite [206](#) anfordert, versucht es, mit einem Computer oder Netzwerk in einer bestimmten Zone zu kommunizieren. Sie können für jedes Programm die folgenden Berechtigungen gewähren oder verweigern:

- Zugriffsrechte für die Sichere Zone
- Zugriffsrechte für die Internetzone
- Serverberechtigung für die Sichere Zone
- Serverberechtigung für die Internetzone.

Indem Sie Zugriffsrechte oder Serverberechtigungen für die Sichere Zone gewähren, ermöglichen Sie es einem Programm, mit Computern und Netzwerken, die Sie in dieser Zone platziert haben, Daten auszutauschen. Dies ist eine äußerst sichere Strategie. Selbst wenn ein Programm manipuliert wird oder versehentlich eine Berechtigung erhält, kann es nur mit einer begrenzten Anzahl an Netzwerken oder Computern Daten austauschen.

Indem Sie eine Zugriffs- oder Serverberechtigung für die Internetzone gewähren, ermöglichen Sie es einem Programm, mit allen beliebigen Computern und Netzwerken Daten auszutauschen.

Konfigurieren neuer Netzwerkverbindungen

Wenn ein Computer an ein Netzwerk angeschlossen ist, können Sie bestimmen, ob dieses Netzwerk der Sicheren Zone oder der Internetzone zugeordnet werden soll.

Wenn Sie ein Netzwerk in die Sichere Zone aufnehmen, können Sie Dateien, Drucker und andere Ressourcen für andere Computer im Netzwerk freigeben. Netzwerke, die Sie kennen und denen Sie vertrauen, wie z.B. Ihr Heimnetzwerk oder Unternehmens-LAN, sollten der Sicheren Zone zugeordnet werden.

Wenn Sie ein Netzwerk der Internetzone zuordnen, können Sie keine Ressourcen für andere Computer des Netzwerks freigeben. Dadurch werden Sie vor Sicherheitsrisiken, die mit der Freigabe von Ressourcen einhergehen, geschützt. Unbekannte Netzwerke sollten der Internetzone zugeordnet werden.

Wenn Ihr Computer eine Verbindung zu einem neuen Netzwerk herstellt, erscheint eine Warnmeldung, die die IP-Adresse des erkannten Netzwerks anzeigt, die standardmäßig der *Internetzone* zugeordnet wird.

Wenn Ihr Computer über einen Proxyserver eine Verbindung zum Internet herstellen soll, fügen Sie den Proxy der Sicheren Zone hinzu. Siehe **Hinzufügen zur Sicheren Zone** auf Seite 87.

Integrieren in Netzwerkdienste

Wenn Sie in einem Heimnetzwerk oder Unternehmens-LAN arbeiten, möchten Sie möglicherweise Dateien, Netzwerkdrucker und andere Ressourcen mit anderen im Netzwerk gemeinsam nutzen oder E-Mails über die Mailserver des Netzwerks

austauschen können. Befolgen Sie die Anweisungen in diesem Abschnitt, um die sichere Ressourcenfreigabe zu aktivieren.

Aktivieren der Datei- und Druckerfreigabe

Um Drucker und Dateien für andere Computer in Ihrem Netzwerk freizugeben, müssen Sie den Endpoint Security Client so konfigurieren, dass der Zugriff auf Computer, mit denen Sie Daten austauschen möchten, zugelassen wird.

So konfigurieren Sie den Client für Datei- und Druckerfreigabe:

1. Fügen Sie das Subnetz des Netzwerks (oder in kleinen Netzwerken die IP-Adresse aller freigegebenen Computer) der Sicherer Zone hinzu.

Siehe *Hinzufügen zur Sicherer Zone* auf Seite [87](#).

2. Stellen Sie die Sicherheitsstufe der Sicherer Zone auf **Mittel** ein. Sichere Computer erhalten damit Zugriff auf Ihre freigegebenen Dateien.

Siehe *Einstellen der Sicherheitsstufen für Zonen*.

3. Stellen Sie die Sicherheitsstufe der Internetzone auf **Hoch** ein. Ihr Computer wird damit von nicht in der Sicherer Zone enthaltenen Computern nicht erkannt.

Herstellen einer Verbindung zu Netzwerk-Mailservern

Endpoint Security Client verwendet automatisch Internet-Mailserver mit den POP3- und IMAP4-Protokollen, wenn Sie Ihrem E-Mail-Client Zugriff auf das Internet gewähren.

Einige Mailserver, wie z. B. Microsoft Exchange, verfügen über Zusammenarbeits- und Synchronisierungsfunktionen, für die der Server als sicher eingestuft werden muss.

So konfigurieren Sie den Client für Mailserver mit Funktionen zur Zusammenarbeit und Synchronisierung:

1. Fügen Sie das Subnetz des Netzwerks oder die IP-Adresse des Mailservers der Sicherer Zone hinzu.
2. Stellen Sie die Sicherheitsstufe der Sicherer Zone auf **Mittel** ein. Die Serverfunktionen zur Zusammenarbeit können jetzt genutzt werden.

3. Stellen Sie die Sicherheitsstufe der Internetzone auf **Hoch** ein. Ihr Computer wird damit von nicht in der Sicheren Zone enthaltenen Computern nicht erkannt.

Aktivieren der gemeinsamen Nutzung einer Internetverbindung ("Internet Connection Sharing", ICS)

Wenn Sie die Windows-Option "Gemeinsame Nutzung einer Internetverbindung (ICS)" verwenden oder ein Programm eines Drittanbieters zur gemeinsamen Nutzung einer Internetverbindung einsetzen, können Sie durch die Installation von Endpoint Security Client nur auf dem Gateway-Computer alle Computer, die die Verbindung gemeinsam nutzen, vor eingehenden Angriffen schützen. Zum Schutz des ausgehenden Datenverkehrs oder zur Anzeige von Warnungen auf den Client-Computern muss Endpoint Security Client jedoch auch auf den Client-Computern installiert sein.

Konfigurieren Sie das Gateway-Client-Verhältnis mit der ICS-Software, bevor Sie den Gateway Client konfigurieren. Wenn Sie statt der ICS-Funktion von Microsoft andere Hardware wie einen Router verwenden, um Ihre Internetverbindung freizugeben, vergewissern Sie sich, dass sich das lokale Subnetz in der Sicheren Zone befindet.

Auswählen der Sicherheitsstufen

Die standardmäßigen Firewall **Sicherheitsstufen** auf Seite [207](#) (Hoch für die Internetzone, Mittel für die Sichere Zone) schützen Ihren Computer vor Portscans und anderer Hackeraktivität; Sie können jedoch weiterhin Drucker, Dateien und andere Ressourcen mit sicheren Computern in Ihrem lokalen Netzwerk gemeinsam verwenden. In den meisten Fällen müssen diese Standardwerte nicht geändert werden. Sobald Endpoint Security Client installiert ist, sind Sie geschützt.

Um die Sicherheitsstufe für eine Zone festzulegen, öffnen Sie **Firewall | Grundeinstellungen** und ziehen die Schieberegler zur gewünschten Einstellung.

Table 0-10 Sicherheit für die Internetzone

HOCH	Dies ist die Standardeinstellung. Ihr Computer befindet sich im Stealth-Modus und wird von anderen Computern nicht erkannt. Der Zugriff auf Windows-Dienste NetBIOS (Network Basic Input/Output System) siehe " NetBIOS " auf Seite 203 sowie die gemeinsame Nutzung von Dateien und Druckern sind gesperrt . Ports sind gesperrt, es sei denn, Sie haben einem Programm die Berechtigung zur Verwendung der Ports erteilt.
------	--

MITTE L	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist zugelassen . Die Programmberechtigungen gelten weiterhin.
NIED RIG	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist zugelassen . Die Programmberechtigungen gelten weiterhin.

Table 0-11 Sicherheit für die Sichere Zone

HOCH	Ihr Computer befindet sich im Stealth-Modus und wird von anderen Computern nicht erkannt. Der Zugriff auf Windows-Dienste (NetBIOS) sowie Datei- und Druckerfreigaben ist gesperrt . Ports sind gesperrt, es sei denn, Sie haben einem Programm die Berechtigung zur Verwendung der Ports erteilt.
MITTE L	Dies ist die Standardeinstellung. Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist zugelassen . Die Programmberechtigungen gelten weiterhin.
NIED RIG	Ihr Computer wird von anderen Computern erkannt. Der Zugriff auf Windows-Dienste sowie Datei- und Druckerfreigaben ist zugelassen . Die Programmberechtigungen gelten weiterhin.

Festlegen von erweiterten Sicherheitsoptionen

Mit erweiterten Sicherheitsoptionen können Sie die Firewall für eine Vielzahl von besonderen Situationen, wie zum Beispiel einem Gateway-Zwang und der gemeinsamen Nutzung einer Internetverbindung (ICS), konfigurieren.

Festlegen von Gateway-Sicherheitsoptionen

In einigen Unternehmen wird bei einem Zugriff auf das Internet die Verwendung von Endpoint Security Client verlangt, wenn dieser über das **Gateway** auf Seite [200](#) des Unternehmens erfolgt. Wenn die Einstellung **Gateway automatisch überprüfen** aktiviert ist, sucht der Client nach allen kompatiblen Gateways und

bestätigt, dass er installiert ist, so dass alle auf die Verwendung des Clients festgelegten Gateways einen Zugriff auf das Internet zulassen.

Sie können die Einstellung dieser Option auch beibehalten, wenn Sie die Verbindung nicht über ein Gateway herstellen. Ihre Internetfunktionen werden dadurch nicht beeinträchtigt.

So legen Sie die automatische Gateway-Überprüfung fest:

1. Öffnen Sie Firewall | Grundeinstellungen.
2. Klicken Sie auf Erweitert.
Das Fenster Erweiterte Einstellungen wird geöffnet.
3. Aktivieren Sie im Bereich Gateway-Sicherheit das Kontrollkästchen Gateway automatisch auf Durchsetzung der Sicherheitsrichtlinien überprüfen .
4. Klicken Sie auf OK.

Festlegen von ICS-Optionen

Wenn Sie **ICS (Internet Connection Sharing)** siehe "ICS" auf Seite 201, verwenden, konfigurieren Sie Endpoint Security Client mit diesen Einstellungen zur Erkennung von ICS-Gateway und Clients.

So legen Sie die Voreinstellungen für die gemeinsame Nutzung der Internetverbindung (ICS) fest:

1. Öffnen Sie Firewall | Grundeinstellungen.
2. Klicken Sie auf Erweitert.
Das Fenster Erweiterte Einstellungen wird geöffnet.
3. Wählen Sie im Bereich Gemeinsame Nutzung der Internetverbindung Ihre Sicherheitseinstellungen aus.
 - Dieser Computer befindet sich nicht in einem ICS/NAT-Netzwerk: Gemeinsame Nutzung der Internetverbindung ist deaktiviert.
 - Dieser Computer ist ein Client eines ICS/NAT-Gateway mit Endpoint Security: Der Client erkennt automatisch die IP-Adresse des ICS-Gateway und zeigt diese im lokalen Gateway Adressfeld an. Sie können die IP-Adresse auch manuell im Feld eingeben.

Durch Aktivieren des Kontrollkästchens **Warnungen des Gateway an diesen Computer weiterleiten** werden Warnungen, die am Gateway auftreten, auf dem Client-Computer angezeigt und protokolliert.

- Dieser Computer ist ein ICS/NAT-Gateway: Der Client erkennt automatisch die IP-Adresse des ICS-Gateway und zeigt diese im lokalen Adressfeld an. Sie können die IP-Adresse auch manuell im Feld eingeben.

Wählen Sie **An Clients weitergeleitete Warnungen lokal unterdrücken** aus, um Warnungen, die vom Gateway an Clients weitergeleitet werden, nicht anzuzeigen.

4. Klicken Sie auf OK.

Festlegen allgemeiner Sicherheitsoptionen

Mit diesen Einstellungen können Sie globale Regeln für bestimmte Protokolle, Pakettypen und andere Formen des Datenverkehrs (z.B. Serververkehr) für die Sichere Zone und die Internetzone angeben.

So ändern Sie die allgemeinen Sicherheitseinstellungen:

1. Öffnen Sie **Firewall | Grundeinstellungen**.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Allgemeine Einstellungen** Ihre Sicherheitseinstellungen aus.

Table 0-12 Allgemeine Einstellungen

Feld	Beschreibung
Alle Fragmente sperren	Sperrt alle unvollständigen (fragmentierten) IP-Datenpakete. Hacker erstellen manchmal fragmentierte Pakete, die Netzwerkgeräte umgehen oder unterbrechen, die Paket-Header lesen. Achtung: Wenn Sie diese Option auswählen, sperrt der Client alle fragmentierten Pakete ohne Warnung und ohne einen Protokolleintrag. Wählen Sie diese Option nur, wenn Sie wissen, wie Ihre Online-Verbindung fragmentierte Pakete behandelt.

Feld	Beschreibung
Sichere Server sperren	Hindert alle Programme auf Ihrem Computer in der Sicheren Zone daran, Serverfunktionen zu übernehmen. Beachten Sie, dass diese Einstellung die im Fenster Programme erteilten Berechtigungen übersteuert.
Internetserver sperren	Hindert alle Programme auf Ihrem Computer in der Internetzone daran, Serverfunktionen zu übernehmen. Beachten Sie, dass diese Einstellung die im Fenster Programme erteilten Berechtigungen übersteuert.
ARP-Schutz aktivieren	Sperrt alle eingehenden ARP-Anfragen, mit Ausnahme von Rundsendungsanfragen an die Adresse des Zielcomputers. Sperrt zudem alle eingehenden ARP-Antworten mit Ausnahme von Antworten auf zuvor ausgegangene ARP-Anfragen.
IP-Datenverkehr über 1394 filtern	Filtert FireWire-Datenverkehr. Bei Wahl dieser Option muss der Computer neu gestartet werden.
VPN-Protokolle zulassen	Ermöglicht den Einsatz von VPN-Protokollen (ESP, AH, GRE, SKIP) selbst bei einer Einstellung mit hoher Sicherheit. Wenn diese Einstellung nicht ausgewählt ist, werden diese Protokolle nur bei mittlerer Sicherheit zugelassen.
Nicht übliche Protokolle bei hoher Sicherheitseinstellung zulassen	Ermöglicht den Einsatz von anderen Protokollen als ESP, AH, GRE und SKIP selbst bei hoher Sicherheitseinstellung.
Hostdatei sperren	Verhindert, dass die Hostdatei Ihres Computers von Hackern unter Einsatz von Spyware oder Trojanern verändert werden kann. Beachten Sie, dass einige vertrauenswürdige Programme die Hostdatei ändern müssen, um korrekt funktionieren zu können.
Deaktivierungsfenster Firewall	Erkennt und deaktiviert Fenster Firewall Diese Option wird nur dann angezeigt, wenn Sie WindowsXP mit Service Pack2 verwenden.

Festlegen von Netzwerk-Sicherheitsoptionen

Mit Hilfe der automatischen Netzwerkerkennung können Sie die Sichere Zone auf einfache Weise so konfigurieren, dass verbreitete Netzwerkaktivitäten wie Datei- und Druckerfreigaben nicht beeinträchtigt werden. Der Client erkennt nur Netzwerke, mit denen Sie physisch verbunden sind. Netzwerke über Router oder virtuelle Netzwerkverbindungen werden nicht erkannt.

Sie können festlegen, ob der Client die erkannten Netzwerke stillschweigend der Sicheren Zone hinzufügt, oder ob Sie jedes Mal gefragt werden sollen, ob ein neu erkanntes Netzwerk hinzugefügt oder abgelehnt werden soll.

So legen Sie Netzwerkeinstellungen fest:

- 1. Öffnen Sie Firewall I Grundeinstellungen.
- 2. Klicken Sie auf Erweitert.
- 3. Wählen Sie im Bereich **Netzwerkeinstellungen** Ihre Sicherheitseinstellungen aus.

Table 0-13 Festlegen von Netzwerk-Einstellungsoptionen

Erkannte Netzwerke zur Sicheren Zone hinzufügen	Fügt der Sicheren Zone automatisch neue Netzwerke hinzu. Diese Einstellung bietet die geringste Sicherheit.
Erkannte Netzwerke von der Sicheren Zone ausschließen	Verhindert automatisch, dass der Sicheren Zone neue Netzwerke hinzugefügt werden, und ordnet diese stattdessen der Internetzone zu. Diese Einstellung bietet die höchste Sicherheit.
Bei neu erkannten Netzwerken Zonenzuweisung erfragen	Der Client zeigt eine Warnung vom Typ Neues Netzwerk oder den Netzwerk-Konfigurationsassistenten an, damit Sie die gewünschte Zone angeben können.

Verwalten von Zonendatenverkehr

Auf der Registerkarte **Zonen** werden die Datenverkehrsquellen (Computer, Netzwerke oder Sites) angezeigt, die Sie der Sicheren Zone oder der Gesperrten Zone zugeordnet haben. Sie enthält darüber hinaus alle Netzwerke, die vom Client erkannt wurden. Wenn Sie an einem einzelnen PC, der nicht mit einem Netzwerk verbunden ist, arbeiten, wird in der Datenverkehrsquellen-Liste nur das Netzwerk Ihres Internetdienstanbieters (ISP) angezeigt, das gewöhnlich der Internetzone zugeordnet wird.

Klicken Sie zum Öffnen der Datenverkehrsquellen-Liste für Zonen auf **Firewall I Zonen**.

Anzeigen von Zonendatenverkehr

In der Datenverkehrsquellen-Liste für Zonen werden die Datenverkehrsquellen und die entsprechenden Zonen angezeigt. Sie können die Liste nach einem beliebigen Feld sortieren, indem Sie auf die jeweilige Spaltenüberschrift klicken. Der Pfeil (^) neben der Überschrift zeigt die Sortierreihenfolge an. Klicken Sie erneut auf dieselbe Überschrift, um die Sortierreihenfolge umzukehren.

Table 0-14 Felder der Datenverkehrsquellen-Liste für Zonen

Feld	Beschreibung
Name	Der von Ihnen dem Computer, Netzwerk oder der Site zugeordnete Name.
IP-Adresse/Site	Die IP-Adresse oder der Hostname der Datenverkehrsquelle.
Eintragstyp	Der Datenverkehrsquellen-Typ: Netzwerk, Host, IP, Site oder Subnetz. Beachten Sie, dass durch das Zulassen oder Sperren des Datenverkehrs für die Datenverkehrsart Host Sicherheitseinstellungen umgangen werden können, besonders in Netzwerken, in denen Hosts dynamisch zugewiesene IP-Adressen erhalten haben.
Zone	Die Zone, der die Datenverkehrsquelle zugeordnet wurde: Internetzone, Sichere Zone oder Gesperrte Zone

Ändern von Zonen-Datenverkehrsquellen

Sie können die Datenverkehrsquelle von der Datenverkehrsquellen-Liste für Zonen aus in eine andere Zone verschieben oder eine Datenverkehrsquelle hinzufügen, bearbeiten oder entfernen.

So ändern Sie die Zone einer Datenverkehrsquelle:

1. Öffnen Sie Firewall | Zonen.
2. Suchen Sie die Datenverkehrsquelle.
3. Klicken Sie in die Spalte **Zonen**, und wählen Sie eine Zone aus.
4. Klicken Sie auf **Übernehmen**.

So fügen Sie eine Datenverkehrsquelle hinzu oder entfernen bzw. bearbeiten diese:

1. Öffnen Sie Firewall | Zonen.
2. Klicken Sie in der Spalte Name auf die Datenverkehrsquelle und anschließend auf **Hinzufügen**, **Bearbeiten** oder **Entfernen**.
3. Klicken Sie auf **Übernehmen**.

Hinzufügen zur Sicheren Zone

Die Sichere Zone umfasst alle Computer, mit denen Sie ohne Bedenken Ressourcen austauschen können. Wenn Sie z.B. drei PCs in einem Ethernet-Heimnetzwerk haben, können Sie entweder jeden einzelnen Computer oder das gesamte Netzwerkadapter-Subnetz der Sicheren Zone zuordnen. Mit der voreingestellten mittleren Sicherheitsstufe der Sicheren Zone können Sie Dateien, Drucker und andere Ressourcen in Ihrem Heimnetzwerk freigeben. Hacker werden auf die Internetzone beschränkt. Dort sorgen die hohen Sicherheitseinstellungen für Ihren Schutz.



Hinweis - Beachten Sie, dass durch das Zulassen oder Sperren des Datenverkehrs für den Datenverkehr des Typs Host Sicherheitseinstellungen umgangen werden können, besonders in Netzwerken, in denen Hosts dynamisch zugewiesene IP-Adressen empfangen haben.

So fügen Sie eine einzelne IP-Adresse hinzu:

1. Öffnen Sie Firewall | Zonen.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie eine IP-Adresse aus.
Das Fenster **IP-Adresse hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie die IP-Adresse und eine Beschreibung an, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK**.

So fügen Sie einen IP-Bereich hinzu:

1. Öffnen Sie Firewall | Zonen.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie eine IP-Adresse aus.
Das Fenster **IP-Bereich hinzufügen** wird angezeigt.

3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie die erste IP-Adresse des Bereichs in das erste und die letzte IP-Adresse des Bereichs in das zweite Feld ein.
5. Geben Sie eine Beschreibung ein.
6. Klicken Sie auf OK.

So fügen Sie ein Subnetz hinzu:

1. Öffnen Sie **Firewall | Zonen**.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie **Subnetz** aus.
Das Dialogfeld **Subnetz hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie die IP-Adresse in das erste und die Subnetz-Maske in das zweite Feld ein.
5. Geben Sie eine Beschreibung ein.
6. Klicken Sie auf OK.

So fügen Sie der Sicheren Zone einen Host oder eine Site hinzu:



Hinweis - Um die IP-Adressen vor dem Hinzufügen der Site anzuzeigen, klicken Sie auf die Schaltfläche **Lookup**. Wenn sich die dem Hostnamen zugewiesenen IP-Adressen ändern, nachdem Sie den Host in die Sichere Zone aufgenommen haben, werden diese IP-Adressen nicht der Sicheren Zone hinzugefügt.

1. Öffnen Sie **Firewall | Zonen**.
2. Klicken Sie auf **Hinzufügen**, und wählen Sie **Host/Site** aus.
Das Fenster **Host/Site hinzufügen** wird angezeigt.
3. Wählen Sie **Sicher** aus der Zonen-Dropdown-Liste aus.
4. Geben Sie den voll qualifizierten Hostnamen im Feld **Hostname** ein.
5. Geben Sie eine Beschreibung für den Host und die Site ein.
6. Klicken Sie auf OK.

Der Client löst den Hostnamen auf, den Sie mit den IP-Adressen eingeben, und fügt diese IP-Adressen der Sicheren Zone hinzu.

So fügen Sie ein Netzwerk zur Sicheren Zone hinzu:

1. Öffnen Sie Firewall | Zonen.
2. Klicken Sie in der Spalte Zone in die Zeile, die das Netzwerk enthält, und wählen Sie anschließend **Sicher**.
3. Klicken Sie auf **Übernehmen**.



Hinweis - Der Client erkennt neue Netzwerkverbindungen automatisch und unterstützt Sie darin, diese der richtigen Zone hinzuzufügen.

Hinzufügen zur Gesperrten Zone

Gehen Sie für das Hinzufügen zur Gesperrten Zone gemäß den Anweisungen zum Hinzufügen zur Sicheren Zone vor. Wählen Sie jedoch **Gesperrt** aus derZone - Dropdown-Liste aus.

Sperren und Freigeben von Ports

Durch die Standard-Sicherheitsstufen des Clients wird festgelegt, welche Ports und Protokolle zugelassen oder gesperrt sind. Wenn Sie ein erfahrener Benutzer sind, können Sie die Definition der Sicherheitseinstellungen ändern, indem Sie die Portberechtigungen ändern und benutzerdefinierte Ports hinzufügen.

Einstellungen für Standard-Portberechtigungen

Die Standardeinstellung für hohe Sicherheit sperrt jeglichen Datenverkehr über Ports, die nicht von Programmen verwendet werden, denen Sie Zugriffsrechte oder Serverberechtigungen erteilt haben. Es gelten die folgenden Ausnahmen:

- DHCP-Rundsendung/Multicast
- Ausgehendes DHCP (Port 67) - in Systemen mit Windows 9x
- Ausgehender DNS (Port 53) - falls der Computer als ein ICS-Gateway konfiguriert ist

Table 0-15 Standard-Zugriffsrechte für Datenverkehrstypen

Datenverkehrstyp	Sicherheitsstufen		
	HOCH	MITTEL	NIEDRIG
DNS, ausgehend	sperren	-	zulassen
DHCP, ausgehend	sperren	-	zulassen
Rundsendung/Multicast	zulassen	zulassen	zulassen
ICMP			
eingehend (Ping-Echo)	sperren	zulassen	zulassen
eingehend (sonstige)	sperren	zulassen	zulassen
ausgehend (Ping-Echo)	sperren	zulassen	zulassen
ausgehend (sonstige)	sperren	zulassen	zulassen
IGMP			
eingehend	sperren	zulassen	zulassen
ausgehend	sperren	zulassen	zulassen
NetBIOS			
eingehend	-	sperren	zulassen
ausgehend	-	zulassen	zulassen
UDP (nicht von einem berechtigten Programm verwendete Ports)			
eingehend	sperren	zulassen	zulassen
ausgehend	sperren	zulassen	zulassen
TCP (nicht von einem berechtigten Programm verwendete Ports)			
eingehend	sperren	zulassen	zulassen

Datenverkehrstyp	Sicherheitsstufen		
	HOCH	MITTEL	NIEDRIG
DNS, ausgehend	sperren	-	zulassen
ausgehend	sperren	zulassen	zulassen

So ändern Sie die Zugriffsrechte für einen Port:

1. Öffnen Sie Firewall | Grundeinstellungen.
2. Klicken Sie im Internetzonenbereich oder im Bereich der Sicheren Zone auf **Benutzerdefiniert**.
Das Fenster Benutzerdefinierte Einstellungen für Firewall wird angezeigt.
3. Blättern Sie zu den Einstellungen für hohe und mittlere Sicherheit.
4. Aktivieren Sie das jeweilige Kontrollkästchen, um einen bestimmten Port oder ein spezifisches Protokoll zu blockieren oder zuzulassen.
5. Klicken Sie auf OK.



Wichtig - Wenn Sie eine Datenverkehrsart in der Einstellungsliste für hohe Sicherheit auswählen, sollten Sie beachten, dass sie dabei **ZULASSEN**, dass diese Datenverkehrsart auch bei hoher Sicherheitsstufe in Ihrem Computer eindringen kann. Sie setzen damit den Schutz herab, der durch die HOHE Sicherheitsstufe gewährt wird. Wenn Sie eine Datenverkehrsart in der Einstellungsliste für mittlere Sicherheit auswählen, sollten Sie beachten, dass Sie durch diese Auswahl diese Datenverkehrsart **SPERREN** und damit den Schutz erhöhen, der durch die Sicherheitsstufe MITTEL gewährt wird.

Hinzufügen benutzerdefinierter Ports

Sie können Kommunikation über zusätzliche Ports bei hoher Sicherheitseinstellung zulassen oder zusätzliche Ports bei mittlerer Sicherheitseinstellung sperren, indem Sie die einzelnen Portnummern oder -bereiche angeben.

So geben Sie zusätzliche Ports an:

1. Öffnen Sie Firewall | Grundeinstellungen.

2. Klicken Sie im Internetzonenbereich oder im Bereich der Sicheren Zone auf **Benutzerdefiniert**.

Das Fenster Benutzerdefinierte Einstellungen für Firewall wird angezeigt.

3. Blättern Sie zu der Sicherheitseinstellung (Hoch oder Mittel), der Sie Ports hinzufügen möchten.
4. Wählen Sie den Porttyp aus, der mit **keine ausgewählt** gekennzeichnet ist: eingehendes UDP, ausgehendes UDP, eingehendes TCP oder ausgehendes TCP.
5. Geben Sie in das Feld **Ports** die Ports oder Portbereiche (durch Kommata getrennt) ein, die Sie freigeben oder sperren möchten. Beispiel: 139, 200-300.
6. Klicken Sie auf OK.

Konfigurieren der VPN-Verbindung für Firewall

Endpoint Security Client ist mit vielen Typen der VPN-Client-Software kompatibel und kann die Verbindung für bestimmte VPN-Clients automatisch konfigurieren.

Unterstützte VPN-Protokolle

Der Client überwacht die in der folgenden Tabelle aufgelisteten VPN-Protokolle.

Table 0-16 Unterstützte VPN-Protokolle

Netzwerkprotokoll	Erklärung und Kommentare
AH	Authentication Header-Protokoll
ESP	Encapsulating Security Payload-Protokoll
GRE	Generic Routing Encapsulation-Protokoll
IKE	Internet Key Exchange-Protokoll
IPSec	IP Security-Protokoll
L2TP	Layer 2 Tunneling Protocol. L2TP ist eine sicherere Variante von PPTP.
LDAP	Lightweight Directory Access Protocol
PPTP	Point-to-Point Tunneling Protocol

Netzwerkprotokoll	Erklärung und Kommentare
SKIP	Simple Key Management for Internet Protocol

Konfigurieren der VPN-Verbindung

Wenn Ihre VPN-Verbindung nicht automatisch konfiguriert werden kann, zeigt der Client die Warnung **Manuelle Maßnahme erforderlich** an, an Hand derer Sie über die erforderlichen manuellen Änderungen zur Konfiguration der Verbindung informiert werden.

Hinzufügen von VPN-Ressourcen zur Sicheren Zone

Sie müssen das VPN-Gateway der Sicheren Zone hinzufügen. Darüber hinaus sind möglicherweise noch andere VPN-bezogene Ressourcen in die Sichere Zone aufzunehmen, damit das VPN richtig funktionieren kann.

Table 0-17 Erforderliche VPN-bezogene Netzwerkressourcen

Erforderliche Ressourcen	Andere Ressourcen
Die folgenden Ressourcen werden von allen VPN-Rechnern benötigt und müssen der Sicheren Zone hinzugefügt werden.	Je nach den Bedingungen Ihrer speziellen VPN-Implementierung sind die unten aufgeführten Ressourcen möglicherweise nicht notwendig.
VPN-Konzentrator	DNS-Server
An den VPN-Client angeschlossene Remote-Hostcomputer (sofern diese nicht in der Subnetzdefinition des Unternehmensnetzwerks enthalten sind).	NIC-Loopback-Adresse des lokalen Hostcomputers (je nach der verwendeten Windows-Version). Wenn für den lokalen Hostcomputer die Loopback-Adresse 127.0.0.1 angegeben wurde, darf auf dem lokalen Host keine Proxy-Software ausgeführt werden.
Subnetze des Unternehmens-Weitbereichsnetzwerks (WAN), auf die der VPN-Client zugreifen soll.	Internet Gateway
Subnetze des Unternehmens-	Lokale Subnetze

Erforderliche Ressourcen	Andere Ressourcen
Die folgenden Ressourcen werden von allen VPN-Rechnern benötigt und müssen der Sicheren Zone hinzugefügt werden.	Je nach den Bedingungen Ihrer speziellen VPN-Implementierung sind die unten aufgeführten Ressourcen möglicherweise nicht notwendig.
LAN, auf die der VPN-Computer zugreifen soll.	Sicherheitsserver (z.B. RADIUS, ACE oder TACACS)

Freigeben des VPN-Gateway

Falls sich das VPN-Gateway in einem gesperrten Bereich oder Subnetz befindet, müssen Sie diesen Bereich oder das Subnetz manuell entsperren.

So heben Sie die Sperre für einen IP-Bereich oder ein Subnetz auf:

1. Öffnen Sie Firewall | Zonen.
2. Wählen Sie in der Spalte Zonen den gesperrten IP-Bereich oder das Subnetz aus.
3. Wählen Sie Sicher aus.
4. Klicken Sie auf Übernehmen.

VPN-Protokolle zulassen

Um sicher zu stellen, dass Ihre VPN-Software mit dem Endpoint Security Client richtig konfiguriert wird, müssen Sie Ihre allgemeinen Sicherheitseinstellungen ändern, um VPN-Protokolle zuzulassen.

So lassen Sie VPN-Protokolle zu:

1. Öffnen Sie Firewall | Grundeinstellungen.
2. Klicken Sie auf Erweitert.
3. Aktivieren Sie im Bereich Allgemein das Kontrollkästchen VPN-Protokolle zulassen.
4. Klicken Sie auf OK.



Hinweis - Sollten in Ihrem VPN andere Protokolle als GRE, ESP oder AH verwendet werden, aktivieren Sie zusätzlich das Kontrollkästchen Nicht übliche Protokolle bei hoher Sicherheit zulassen

Gewähren von Zugriffsrechten für VPN-Software

Gewähren Sie dem VPN-Client und allen anderen VPN-bezogenen Programmen Zugriffsrechte.

So gewähren Sie Ihren VPN-Programmen Zugriffsrechte:

1. Öffnen Sie Program ControllProgramme.
2. Wählen Sie in der Spalte Programme ein VPN-Programm aus.
3. Klicken Sie in der Spalte Zugriff unterhalb von Sicher, und wählen Sie Zulassen aus.



Hinweis - Falls Ihr VPN-Programm nicht aufgeführt ist, klicken Sie auf Hinzufügen , um das Programm der Liste hinzuzufügen.

So gewähren Sie VPN-bezogenen Komponenten Zugriffsrechte:

1. Öffnen Sie Program ControllKomponenten.
2. Wählen Sie in der Spalte Komponenten die VPN-Komponente aus, die Zugriffsrechte erhalten soll.
3. Wählen Sie in der Spalte Zugriff die Einstellung Zulassen aus.

Program Control

Program Control schützt Ihren Computer, indem sicher gestellt wird, dass nur diejenigen Programme auf das Internet zugreifen können, die Sie als vertrauenswürdig einstufen. Zur Konfiguration der Programmmzugriffsrechte können Sie bei Bedarf die Programmwarnungen verwenden, oder Sie können gleich von Anfang an die entsprechenden Berechtigungen in der Registerkarte **Programme** einrichten. Erfahrene Benutzer können auch die Ports festlegen, zu deren Nutzung die einzelnen Programme berechtigt sind.

Inhalt dieses Abschnitts

Grundlegendes zu Program Control	97
Festlegen der Optionen von Program Control	98
Konfigurieren des Programmmzugriffs	101
Einstellen spezifischer Berechtigungen	103
Verwalten von Programmkomponenten	108
Verwenden von Programmen mit dem Client	109

Grundlegendes zu Program Control

Um Ihren Computer vor Malware zu schützen, verwenden die Funktionen von Program Control die Programmauthentifizierung (überprüft, ob die Programme manipuliert wurden) und die Programmmzugriffssteuerung (vergibt nur auf Ihren Befehl hin Zugriffsrechte oder Serverberechtigungen).

Zugriffssteuerung für Programme

Wenn ein Programm zum ersten Mal Zugriffsrechte anfordert, wird die Warnung "Neues Programm" angezeigt, und Sie werden gefragt, ob Sie diesem Programm Zugriffsrechte erteilen möchten. Wenn das Programm versucht, als Server zu

fungieren, wird die Warnung **Serverprogramm** angezeigt. In einer Serverprogrammwarnung werden Sie gefragt, ob Sie einem Programm eine Serverberechtigung erteilen möchten.

Damit nicht immer wieder zahlreiche Warnungen für das gleiche Programm angezeigt werden, aktivieren Sie das Kontrollkästchen **Diese Einstellung beim nächsten Start des Programms verwenden**, bevor Sie auf Ja oder Nein klicken.

Anschließend wird das Programm vom Client im Hintergrund gesperrt bzw. zugelassen. Wenn das gleiche Programm erneut Zugriffsrechte anfordert, wird die Warnung bei bekannten Programmen angezeigt, und Sie werden gefragt, ob Sie einem Programm, das bereits zuvor Zugriffsrechte angefordert hat, diese erteilen oder verweigern möchten.

Erteilen Sie nur solchen Programmen Serverberechtigungen, die Sie als vertrauenswürdig einstufen und die für ihre ordnungsgemäße Funktion Serverberechtigungen benötigen. Trojaner und andere Malware sind häufig auf Serverberechtigungen angewiesen.

Programmauthentifizierung

Wenn ein Programm auf Ihrem Computer versucht, auf das Internet zuzugreifen, wird es von Endpoint Security Client mithilfe der Funktion Smart-Prüfsumme authentifiziert. Falls das Programm seit dem letzten Internetzugriff geändert wurde, zeigt der Client die Warnung bei Änderung eines Programms an.

Sie entscheiden dann, ob dem Programm Zugriff gewährt werden soll. Für zusätzliche Sicherheit authentifiziert der Client außerdem die Komponenten, z. B. **DLL** auf Seite 199-Dateien, die mit der ausführbaren Datei des Programms verknüpft sind. Wenn eine Komponente seit der letzten Berechtigungserteilung geändert wurde, zeigt der Client die Warnung für Programmkomponente an, die in ihrer Erscheinung der Warnung bei Änderung eines Programms entspricht.

Festlegen der Optionen von Program Control

Bei Verwendung von Endpoint Security Client kann kein Programm auf Ihrem Computer ohne Ihre Erlaubnis auf das Internet oder Ihr lokales Netzwerk zugreifen oder Serverfunktionen bereitstellen.

Festlegen der Sicherheitsstufe für Program Control

Verwenden Sie die Sicherheitsstufe für Program Control, um die Anzahl der Programmwarnungen zu regulieren, die beim ersten Einsatz des Clients angezeigt werden.

Check Point empfiehlt für die ersten Tage des normalen Betriebs die Einstellung für mittlere Sicherheit. Mit dem *Komponenten-Lernmodus* kann sich der Client schnell mit den MD5-Signaturen häufig verwendeter Komponenten vertraut machen, ohne Ihre Arbeit durch zahlreiche Warnungen zu unterbrechen. Verwenden Sie diese Einstellung so lange, bis Sie alle Internet-Anwendungen (z. B. Browser, E-Mail-Client und Chat-Programme) mindestens ein Mal bei laufendem Client ausgeführt haben. Nachdem Sie alle Programme, die Internetzugriff benötigen, ein Mal verwendet haben, stellen Sie die Sicherheitsstufe in den Einstellungen von Program Control auf Hoch.

So legen Sie die globale Sicherheitsstufe für Program Control fest:

1. Öffnen Sie Program Control | Grundeinstellungen.
2. Klicken Sie im Bereich Program Control auf den Schieberegler, und ziehen Sie ihn zur gewünschten Einstellung.

Table 0-18 Sicherheitsstufe für Program Control

HOCH	Die erweiterten Programm- und Komponenteneinstellungen sowie die Interaktionssteuerung für Anwendung sind aktiviert. Eventuell werden Ihnen zahlreiche Warnungen angezeigt. Programme und Komponenten werden authentifiziert. Programmberechtigungen werden durchgesetzt, und die Interaktionssteuerung für Anwendungen ist aktiviert.
MITTE L	Die erweiterten Einstellungen für Program Control sowie die Interaktionssteuerung für Anwendung sind deaktiviert. Es werden weniger Warnungen angezeigt. Lernmodus für Komponenten ist aktiviert. Programme werden authentifiziert; Komponenten werden erlernt. Programmberechtigungen werden erzwungen. Hinweis: Nachdem Sie alle Programme, die Internetzugriff benötigen, einmal verwendet haben, setzen Sie die Sicherheitsstufe in den Einstellungen für Program Control auf Hoch.

NIEDRIG	Erweiterte Einstellungen für Program Control sind deaktiviert. Der Lernmodus für Komponenten und Programme ist aktiviert. Es werden keine Programmwarnungen angezeigt.
AUS	Program Control ist deaktiviert. Programme und Komponenten werden weder authentifiziert noch erlernt. Es werden keine Programmberechtigungen erzwungen. Allen Programmen werden Zugriffsrechte und Serverberechtigungen gewährt. Es werden keine Programmwarnungen angezeigt.

Aktivieren der automatischen Sperre

Die automatische Internetsperre schützt Ihren Computer, wenn Sie für einen längeren Zeitraum eine Verbindung mit dem Internet aufrechterhalten, auch wenn Sie nicht aktiv auf Netzwerk- oder Internetressourcen zugreifen.

Bei aktivierter Sperre wird nur Datenverkehr zugelassen, der von Programmen gesendet wird, denen Sie eine Berechtigung zur Umgehung der Internetsperre erteilt haben. Jeglicher Datenverkehr vom und zum Rechner wird unterbunden, darunter auch DHCP-Nachrichten oder ISP-Heartbeat-Signale, die zur Aufrechterhaltung Ihrer Internetverbindung verwendet werden. In der Folge wird Ihre Internetverbindung möglicherweise getrennt.

Sie können die Internetsperre so festlegen, dass sie aktiviert wird, wenn:

- der Bildschirmschoner aktiviert wird oder
- wenn eine bestimmte Zeit (in Minuten) lang keine Netzwerkaktivität stattfindet.

So aktivieren oder deaktivieren Sie die automatische Sperre:

1. Öffnen Sie Program Control | Grundeinstellungen.
2. Wählen Sie im Bereich Automatische Sperre die Option Ein oder Aus.

So legen Sie die Optionen für die automatische Sperre fest:

1. Öffnen Sie Program Control | Grundeinstellungen.
2. Klicken Sie im Bereich Automatische Sperre auf Benutzerdefiniert.

Das Fenster Einstellungen für benutzerdefinierte Sperre wird angezeigt.

3. Geben Sie den zu verwendenden Sperrmodus an:

- **Sperren nach __ Minuten Inaktivität:** Aktiviert die automatische Sperre nach Ablauf der in Minuten angegeben Zeit. Geben Sie einen Wert zwischen 1 und 99 ein.
- **Sperren bei Aktivierung des Bildschirmschoners:** Aktiviert die automatische Sperre, wenn der Bildschirmschoner aktiviert wird.

Konfigurieren des Programmzugriffs

Sie können den Programmzugriff automatisch oder manuell konfigurieren. Mithilfe des Programmassistenten können Sie den Internetzugriff für einige der gängigsten Programme automatisch konfigurieren.

Einstellen der Zugriffsrechte für Programme

Der Endpoint Security Client zeigt die Warnung Neues Programm an, wenn ein Programm auf Ihrem Computer zum ersten Mal Zugriff auf das Internet oder lokale Netzwerkressourcen anfordert. Die Warnung "Serverprogramm" wird angezeigt, wenn ein Programm zum ersten Mal versucht, Serverfunktionen auszuführen. Sie können den Client so konfigurieren, dass neue Programme ohne Anzeigen einer Warnung zugelassen oder gesperrt werden. Wenn Sie z.B. sicher sind, dass Sie allen gewünschten Programmen die nötigen Zugriffsrechte erteilt haben, können Sie die Software so konfigurieren, dass keinen anderen Programmen Zugriffsrechte erteilt werden.

So legen Sie die Verbindungsversuchsberechtigungen für neue Programme fest:

1. Öffnen Sie Program Control Grundeinstellungen.
2. Klicken Sie auf Erweitert.

Das Fenster Erweiterte Einstellungen wird geöffnet.

3. Wählen Sie im Bereich Verbindungsversuche Ihre Voreinstellungen für jede Zone aus.

Table 0-19 Verbindungsversuche

Zugriff immer gewähren	Gewährt allen neuen Programmen Zugriff auf die angegebene Zone.
Zugriff immer verweigern	Verweigert allen Programmen Zugriff auf die angegebene Zone.

Immer fragen

Zeigt eine Warnung an, in der für das Programm Zugriffsrechte auf die angegebene Zone angefordert werden.



Hinweis - Einstellungen für einzelne Programme können auf der Registerkarte Programme vorgenommen werden. Die Einstellungen in diesem Bildschirm gelten NUR für Programme, die noch nicht in der Registerkarte Programme aufgeführt sind.

So legen Sie die Serverversuchsberechtigungen für neue Programme fest:

1. Öffnen Sie Program Control | Grundeinstellungen.
2. Klicken Sie auf **Erweitert**.
3. Wählen Sie im Bereich **Serverversuche** Ihre Voreinstellungen für jede Zone aus.

Table 0-20 Serverversuche

Verbindung immer annehmen	Berechtigt alle Programme dazu, als Server zu fungieren.
Verbindung immer ablehnen	Verweigert es allen Programmen, als Server zu fungieren.
Immer fragen	Zeigt eine Warnung an, in der Sie gefragt werden, ob das Programm als Server fungieren kann.

Anpassen der Einstellungen von Program Control

Der Client fragt Sie standardmäßig, ob Verbindungsversuche und Serverzugriffsversuche für die Internetzone und Sichere Zone zugelassen oder gesperrt werden sollen. Falls der TrueVector-Dienst ausgeführt wird, der Client jedoch nicht, wird der Programmzugriff standardmäßig verweigert.

Sie können Program Control anpassen, indem Sie globale Programmeigenschaften festlegen.

So legen Sie die globalen Programmeigenschaften fest:

1. Öffnen Sie Program Controll Grundeinstellungen.
2. Klicken Sie auf **Erweitert**, und öffnen Sie die Registerkarte **Warnungen & Funktionen**.
3. Geben Sie globale Programmooptionen an.

Table 0-21 Globale Programmooptionen

Bei verweigertem Internetzugriff Meldung anzeigen	Zeigt eine Warnung bei gesperrten Programmen an, wenn der Client einem Programm den Zugriff verweigert. Deaktivieren Sie diese Option, wenn der Zugriff ohne Anzeigen einer Warnung verweigert werden soll.
Zugriff verweigern, wenn die Option „Fragen“ gewählt wurde und der TrueVector-Dienst ohne Client ausgeführt wird:	Schützt die Client-Anwendung vor dem seltenen Fall, dass ein unabhängiger Prozess (z.B. ein Trojaner) den Client beendet, der TrueVector-Dienst jedoch weiterhin ausgeführt wird.
Programmen nur mit Kennwort zeitweiligen Internetzugriff gewähren	Fordert Sie auf, ein Kennwort einzugeben, damit Zugriffsrechte erteilt werden können. Sie müssen angemeldet sein, um auf eine Programmwarnung mit Ja antworten zu können. Damit der Zugriff ohne Kennwort gewährt wird, deaktivieren Sie diese Option.

Einstellen spezifischer Berechtigungen

Durch Einstellen der Sicherheitsstufen für Program Control auf **Hoch**, **Mittel** oder **Niedrig** geben Sie global an, ob Programme und deren Komponenten Zugriffsrechte anfordern müssen, bevor sie auf das Internet zugreifen oder Serverfunktionen ausführen können.

Sie können auch spezifische Einstellungen für ein einzelnes Programm angeben. Wenn Sie z.B. einem bestimmten Programm Zugriffsrechte gewähren möchten, die Sicherheitsstufe für alle anderen Programme jedoch auf **Hoch** belassen möchten, können Sie die Berechtigung für dieses Programm auf **Zulassen** setzen.

Verwenden der Programmliste

Die Programmliste enthält die Programme, die versucht haben, auf das Internet oder lokale Netzwerk zuzugreifen. Außerdem wird angezeigt, in welcher Zone sich das Programm befindet, ob es als Server fungieren und ob es E-Mail-Nachrichten senden kann. Während Sie mit Ihrem Computer arbeiten, erkennt der Client alle Programme, die Netzwerkzugriff anfordern, und fügt sie dieser Liste hinzu.

So greifen Sie auf die Programmliste zu:

Öffnen Sie Program Control | Programme.

Die Spalten **Zugriff**, **Server** und **Mail senden** geben an, ob ein bestimmtes Programm über die nötigen Rechte verfügt, um auf das Internet zuzugreifen, als Server zu fungieren oder E-Mail-Nachrichten zu senden.

Table 0-22 Symbole für Programm-Zugriffsberechtigungen

Symbol	Bedeutung
	Dem Programm werden Zugriffs- und Serverrechte gewährt. Um die Berechtigung zu ändern, klicken Sie auf das Symbol, und wählen Sie entweder Sperren oder Fragen aus.
	Der Client zeigt eine Programmwarnung an, wenn das Programm Zugriffs- bzw. Serverrechte anfordert. Um die Berechtigung zu ändern, klicken Sie auf das Symbol, und wählen Sie entweder Zulassen oder Sperren .
	Dem Programm werden keine Zugriffs- oder Serverrechte gewährt. Um die Berechtigung zu ändern, klicken Sie auf das Symbol, und wählen Sie entweder Zulassen oder Fragen aus.
	Das Programm ist derzeit aktiv.

Hinzufügen von Programmen zur Programmliste

Wenn Sie Zugriffsrechte oder Serverberechtigungen für ein Programm angeben möchten, das sich nicht in der Programmliste befindet, können Sie das Programm der Liste hinzufügen und Berechtigungen festlegen.

So fügen Sie ein Programm zur Programmliste hinzu:

1. Öffnen Sie **Program Control | Programme**.
2. Klicken Sie auf **Hinzufügen**.
Das Fenster **Programm hinzufügen** wird angezeigt.
3. Wählen Sie das hinzuzufügende Programm aus, und klicken Sie auf **Öffnen**.
Wählen Sie die ausführbare Datei des Programms aus.

So bearbeiten Sie ein Programm in der Programmliste:

1. Öffnen Sie **Program Control | Programme**.

2. Klicken Sie mit der rechten Maustaste in die Spalte **Programme** , und wählen Sie eine der Optionen aus.

Table 0-23 Optionen von Program Control

Veränderung Häufigkeit	Der Client authentifiziert das Programm nur an Hand der Dateipfadinformationen. Die MD5-Signatur wird nicht überprüft. Achtung: Diese Einstellung gewährleistet nur geringe Sicherheit.
Optionen	Öffnet das Dialogfeld Programmooptionen , in dem Sie Sicherheitsoptionen anpassen und erweiterte Regeln für Programme erstellen können.
Eigenschaften	Öffnet das Dialogfeld Eigenschaften des Betriebssystems für das entsprechende Programm.
Entfernen	Löscht das Programm aus der Liste.

Gewähren von Internet-Zugriffsrechten für Programme

Es gibt verschiedene Möglichkeiten, einem Programm Zugriffsrechte für das Internet zu gewähren: mit einer Reaktion auf eine Warnung, durch manuelle Konfiguration in der Programmliste und durch automatische Konfiguration mithilfe des Clients.

Viele der häufig verwendeten Programme können automatisch für den sicheren Internetzugriff konfiguriert werden. Sie können feststellen, ob ein Programm manuell oder automatisch konfiguriert wurde, indem Sie das Programm in der Programmliste auswählen und im Feld **Detailinformationen für Eintrag** nachsehen.

So gewähren Sie einem Programm die Berechtigung zum Zugriff auf das Internet:

1. Öffnen Sie **Program Control | Programme**.
2. Klicken Sie in der Spalte **Programme** auf das Programm, und wählen Sie **Zulassen** aus.

Integrierte Regeln gewährleisten konsistente SicherheitsRichtlinie für alle Programme. Programme mit Zugriff auf die Internetzone haben auch Zugriff auf die Sichere Zone. Programme mit Serverberechtigung in einer Zone haben auch Zugriffsrechte für diese Zone. Wenn Sie beispielsweise **Allow under Trusted Zone/Server** (für Sichere Zone oder Server zulassen) auswählen, werden automatisch auch alle anderen Berechtigungen für das Programm auf Zulassen gesetzt.

Erteilen der Serverberechtigung für Programme

Gehen Sie vorsichtig vor, wenn Sie Programmen die Berechtigung gewähren, als Server zu fungieren, da Trojaner und andere Typen von Malware oft Serverberechtigungen benötigen. Die Berechtigung, als Server zu fungieren, sollte Programmen vorbehalten bleiben, die Sie kennen, denen Sie vertrauen, und die auf die Serverberechtigung angewiesen sind, um richtig funktionieren zu können.

So gewähren Sie einem Programm die Berechtigung, als Server zu fungieren:

1. Öffnen Sie Program Control | Programme.
2. Klicken Sie in der Spalte Programme auf das Programm, und wählen Sie Zulassen aus.

Erteilen der Berechtigung zum Senden von E-Mails für Programme

Damit Ihr E-Mail-Programm E-Mail-Nachrichten senden kann und um den Schutz vor Bedrohungen durch E-Mails zu aktivieren, gewähren Sie Ihrem E-Mail-Programm die Berechtigung Mail senden.

So gewähren Sie einem Programm die Berechtigung "Mail senden":

1. Öffnen Sie Program Control | Programme.
2. Klicken Sie in der Liste in die Spalte Mail senden des Programms, und wählen Sie Zulassen aus.

Erweiterte Einstellungen für Program Control

Die erweiterten Einstellungen für Program Control erhöhen die Sicherheit, da sie verhindern, dass unbekannte Programme sichere Programme für den Zugriff auf das Internet verwenden, und Hacker daran hindern, Ihren Computer mit der CreateProcess- und OpenProcess-Funktion von Windows zu manipulieren.

Die folgenden Anwendungen dürfen standardmäßig über andere Programme auf das Internet zugreifen:

- Endpoint Security
- MS Word, Excel, PowerPoint und Outlook

So aktivieren Sie die erweiterten Program Control-Einstellungen für ein Programm:

1. Öffnen Sie Program Control | Programme.
2. Wählen Sie in der Spalte Programme ein Programm aus.
3. Klicken Sie auf Optionen.

Das Fenster Programmoptionen wird angezeigt.

4. Öffnen Sie die Registerkarte Sicherheit.
5. Legen Sie die erweiterten Optionen von Program Control fest:

Table 0-24 Erweiterte Einstellungen für Program Control

Dieses Programm darf andere Programme für den Zugriff auf das Internet verwenden	Ermöglicht es dem ausgewählten Programm, über andere Programme auf das Internet zuzugreifen
Anwendungsinteraktion zulassen	Ermöglicht es dem ausgewählten Programm, die Funktionen OpenProcess und CreateProcess auf Ihrem Computer zu verwenden.

Deaktivieren des Schutzes für ausgehende E-Mails

Der Schutz für ausgehende E-Mails ist standardmäßig für alle Programme aktiviert. Da die Möglichkeit zum Senden von E-Mails nicht bei allen Programme gegeben ist, können Sie den Schutz für ausgehende E-Mails für jedes Programm deaktivieren, bei dem dies nicht erforderlich ist.

So deaktivieren Sie die Schutzfunktion für ausgehende E-Mails für ein Programm:

1. Öffnen Sie Program Control | Programme.
2. Wählen Sie ein Programm in der Liste aus, und klicken Sie anschließend auf Optionen.

Das Fenster Programmoptionen wird angezeigt.

3. Öffnen Sie die Registerkarte Sicherheit.
4. Deaktivieren Sie das Kontrollkästchen Schutz für ausgehende E-Mail für dieses Programm aktivieren .

Einstellen der Authentifizierungsoptionen

Alle Programme werden standardmäßig über ihre Komponenten authentifiziert. Im Fenster Programmooptionen können Sie Authentifizierungsoptionen für ein Programm festlegen.

Zulassen der Verwendung von Programmen durch andere Benutzer

Sie möchten möglicherweise verhindern, dass Ihre Kinder Ihre Sicherheitseinstellungen ändern, ihnen jedoch trotzdem die Verwendung neuer Programme erlauben.

So gewähren Sie Zugriff auf Programme ohne ein Kennwort:

1. Öffnen Sie Überblick | Voreinstellungen.
2. Klicken Sie auf Kennwort festlegen.
3. Aktivieren Sie das Kontrollkästchen **Andere Benutzer können Programme ohne ein Kennwort verwenden** (außer wenn die Programmmzugriffsberechtigung auf "Sperren" eingestellt ist).

Wenn diese Option aktiviert ist, müssen Benutzer ein Kennwort angeben, bevor sie Einstellungen ändern können. Die Benutzer sind jedoch berechtigt, neuen Programmen und Programmen, für die die Berechtigung "Fragen" festgelegt wurde, ohne Angabe des Kennworts Internetzugriff zu gewähren. Der Zugriff auf Programme, die Sie ausdrücklich gesperrt haben, wird verweigert.

4. Klicken Sie auf OK.

Verwalten von Programmkomponenten

Sie können für jedes Programm auf Ihrem Computer angeben, ob der Client nur die Programmdatei selbst oder auch die verwendeten Komponenten der Authentifizierung unterzieht. Darüber hinaus können Sie einzelnen Programmkomponenten den Zugriff gewähren oder verweigern.

Die Komponentenliste enthält die Programmkomponenten für zugelassene Programme, die versucht haben, auf das Internet oder lokale Netzwerk zuzugreifen. In der Spalte **Zugriff** wird angegeben, ob der Komponente immer Zugriff gewährt wird oder ob der Client Sie warnen soll, wenn diese Komponente versucht, auf das Internet oder das lokale Netzwerk zuzugreifen.

Während Sie mit Ihrem Computer arbeiten, erkennt der Client die Komponenten, die von Ihren Programmen verwendet werden, und fügt sie der Komponentenliste hinzu.

So greifen Sie auf die Komponentenliste zu:

1. Öffnen Sie Program Control | Komponenten.

So gewähren Sie einer Programmkomponente Zugriffsrechte:

1. Öffnen Sie Program Controll Komponenten.
2. Wählen Sie in der Liste eine Komponente aus, klicken Sie in die Spalte Zugriff, und wählen Sie Zulassen aus.

Verwenden von Programmen mit dem Client

Um sicher zu stellen, dass Ihre anderen Softwareprogramme mit dem Client kompatibel sind, müssen Sie möglicherweise die Konfigurationseinstellungen des Programms ändern.

Viele der häufig verwendeten Programme können automatisch für den Internetzugriff konfiguriert werden. An Hand der Liste im Programmassistenten können Sie erkennen, ob das Programm, das Sie verwenden, automatisch konfiguriert werden kann. In einigen Fällen kann der Zugriff auf das Internet automatisch konfiguriert werden. Viele Programme benötigen jedoch zusätzlich Serverzugriffsrechte.

Verwenden von Antivirus-Software

Damit Ihre Antivirus-Software aktualisiert werden kann, muss sie über Zugriffsrechte für die Sichere Zone verfügen.

Um Aktualisierungen vom Hersteller Ihres Antivirus-Programms beziehen zu können, fügen Sie die Domäne, die die Aktualisierungen enthält (z.B. update.avsupdate.com), Ihrer Sicheren Zone hinzu. Siehe **Hinzufügen zur Sicheren Zone** auf Seite [87](#).

Verwenden von Browsern

Ein Browser benötigt für den reibungslosen Betrieb Zugriffsrechte für die Internetzone und die Sichere Zone. Achten Sie auf die optimale Einstellung der

Sicherheitsfunktionen Ihres Browsers, und installieren Sie stets die aktuellsten Service Packs für Ihren Browser, bevor Sie Berechtigungen gewähren.

Führen Sie eine der folgenden Optionen aus, um Ihrem Browser Zugriffsrechte zu gewähren:

- Führen Sie den Programmassistenten aus.
Der Client erkennt automatisch Ihren Standardbrowser und fordert Sie auf, diesem Zugriffsrechte für die Internetzone zu gewähren.
- Erteilen Sie dem Programm direkt Zugriffsrechte. Siehe ***Gewähren von Internet-Zugriffsrechten für Programme*** auf Seite [105](#).
Antworten Sie mit Ja , wenn eine Programmwarnung für den Browser angezeigt wird.

Verwenden von Chat-Programmen

Programme für Chat und Instant Messaging (z.B. AOL Instant Messenger) benötigen unter Umständen Serverberechtigungen, damit sie ordnungsgemäß funktionieren.

So gewähren Sie Ihrem Chat-Programm Zugriffsrechte:

- Klicken Sie in der Warnung **Serverprogramm** auf Ja.
- Erteilen Sie dem Programm Serverberechtigungen.

Siehe ***Erteilen der Serverberechtigung für Programme*** auf Seite [106](#).



Wichtig - Es wird dringend empfohlen, keine unbestätigten Dateiübertragungen durch Chat-Programme zuzulassen.

Verwenden von E-Mail

Damit ein E-Mail-Programm Mails senden und empfangen kann, benötigt es Zugriffsrechte für die Zone, in der sich der Mailserver befindet. Außerdem können manche E-Mail-Clients mehrere Komponenten enthalten, die Serverberechtigungen erfordern. So müssen z.B. bei Microsoft Outlook sowohl die Basisanwendung (OUTLOOK.EXE) als auch der Spooler für das Messaging-Subsystem (MAPI32.EXE) über Serverberechtigungen verfügen.

So gewähren Sie E-Mail-Programmen sicheren Zugriff:

1. Fügen Sie den lokalen Mailserver der Sicheren Zone hinzu.
2. Beschränken Sie den Zugriff des E-Mail-Programms auf die Sichere Zone.
3. Fügen Sie den Remote-Mailserver (Host) der Sicheren Zone hinzu.



Hinweis - Sie können die Sicherheit auch erhöhen, indem Sie die Anzahl der Ports, die Ihr E-Mail-Programm verwenden darf, einschränken (siehe **Default Port Permission Settings** siehe "[Einstellungen für Standard-Portberechtigungen](#)" auf Seite 89) (Einstellungen für Standard-Portberechtigungen).

Verwenden von internetbasierten Anrufbeantworterdiensten

So verwenden Sie internetbasierte Anrufbeantworterprogramme (z.B. CallWave) zusammen mit dem Client:

1. Erteilen Sie dem Programm Serverberechtigungen und Zugriffsrechte für die Internetzone.
2. Fügen Sie die IP-Adresse der Server des Anbieters der Sicheren Zone hinzu.
3. Setzen Sie die Sicherheitsstufe für die Internetzone auf **Mittel**.



Hinweis - Wenden Sie sich an den technischen Kundendienst des Anbieters, um die IP-Adresse der Server herauszufinden.

Verwenden von Filesharing

Filesharing-Programme wie Napster, Limewire, AudioGalaxy oder Gnutella-Clients benötigen für die Zusammenarbeit mit dem Client Serverberechtigungen für die Internetzone.

Verwenden von FTP

Zur Verwendung von FTP-Programmen (File Transfer Protocol) müssen Sie möglicherweise die Einstellungen Ihres FTP-Client-Programms anpassen.

So aktivieren Sie FTP mit dem Client:

1. Aktivieren Sie auf Ihrem FTP-Client den passiven Modus PASV.

Dieser bestimmt, dass der Client für beide Richtungen der Datenübertragung denselben Port verwendet. Wenn PASV nicht aktiviert ist, sperrt der Client

möglicherweise die Versuche des FTP-Servers, eine Verbindung zu einem neuen Port für die Datenübertragung herzustellen.

2. Fügen Sie die verwendeten FTP-Sites zur Sicherer Zone hinzu.
3. Erteilen Sie Ihrem FTP-Client-Programm Zugriffsrechte für die Sichere Zone.

Weitere Informationen zum Hinzufügen zur Sicherer Zone und dem Erteilen von Zugriffsrechten für ein Programm finden Sie unter **Setting Advanced Security Options** siehe "[Festlegen von erweiterten Sicherheitsoptionen](#)" auf Seite [81](#) (Festlegen von erweiterten Sicherheitsoptionen).

Verwenden von Streaming Media

Damit der Client zusammen mit Anwendungen funktioniert, bei denen Audio- und Videodaten abgespielt werden (z. B. RealPlayer, Windows Media Player, QuickTime usw.), müssen die betreffenden Anwendungen über Serverberechtigungen für die Internetzone verfügen.

Weitere Informationen dazu, wie Sie einem Programm Serverberechtigungen erteilen, finden Sie unter **Erteilen der Serverberechtigung für Programme** auf Seite [106](#).

Verwenden von Spielen

Wenn Sie während der Verwendung des Clients Internetspiele spielen möchten, müssen Sie unter Umständen die Programm-Zugriffsberechtigungen und Sicherheitsstufen anpassen.

Verwenden der Fernsteuerung

Konfigurieren Sie die Fernsteuerung, wenn Ihr Computer Host oder Client eines RAS-Systems (Remote Access System) wie PCAnywhere oder Timbuktu ist.

So konfigurieren Sie den Remote-Zugriff:

1. Fügen Sie die IP-Adressen der Hosts oder Clients der Sicherer Zone hinzu. Siehe **Hinzufügen zur Sicherer Zone** auf Seite [87](#).
2. Fügen Sie das Subnetz des Netzwerks, für das der Remote-Zugriff hergestellt wird, der Sicherer Zone hinzu.

3. Wenn dem Remote-Computer eine dynamische IP-Adresse zugewiesen ist, fügen Sie die betreffenden DHCP-Serveradressen der Sicheren Zone hinzu.



Wichtig – Wenn der Remote-Control-Client oder -Host sich in einem Netzwerk befinden, das nicht Ihrer Kontrolle unterliegt, wird die Verbindungsherstellung möglicherweise durch umgebende Firewalls oder andere Netzwerkfunktionen verhindert.

Verwenden von VNC

So aktivieren Sie VNC und Endpoint Security für die gleichzeitige Verwendung:

1. Führen Sie auf dem Server und dem Client einen der folgenden Schritte aus:

- Wenn Sie die IP-Adresse oder das Subnetz des Viewers (Client) kennen, den Sie für den Remote-Zugriff verwenden, und die IP-Adresse bzw. das Subnetz immer gleich ist, fügen Sie die Adresse oder das Subnetz der Sicheren Zone hinzu. Siehe ***Hinzufügen zur Sicheren Zone*** auf Seite [87](#).
- Wenn Sie die IP-Adresse des Viewers nicht kennen oder sich diese ändert, gewähren Sie dem Programm Zugriffsrechte und Serverberechtigungen für die Sichere Zone und die Internetzone. Siehe ***Einstellen spezifischer Berechtigungen*** auf Seite [103](#).

Wenn die entsprechende Aufforderung von VNCviewer auf dem Viewer angezeigt wird, geben Sie den Namen oder die IP-Adresse des Servers und danach das Kennwort ein. Sie können jetzt eine Verbindung herstellen.

2. Führen Sie auf dem Viewer (Client) VNCviewer aus, um eine Verbindung zum Server herzustellen. Führen Sie das Programm nicht im Modus zum Überwachen von Verbindungsanforderungen aus.



Wichtig – Wenn Sie den VNC-Zugriff aktivieren, indem Sie Serverberechtigungen und Zugriffsrechte gewähren, richten Sie auf jeden Fall ein VNC-Kennwort ein, und verwenden Sie dieses, damit die Sicherheit gewährleistet ist.

Es wird empfohlen, die IP-Adressen des Servers und Viewers der Sicheren Zone hinzuzufügen, statt der Anwendung Zugriffsrechte für die Internetzone zu gewähren.

Verwenden von Voice over IP (VoIP)

Wenn Sie den Client zusammen mit VoIP-Programmen (Voice over IP) verwenden möchten, müssen Sie je nach Programm einen oder beide der folgenden Schritte ausführen:

1. Gewähren der VoIP-Anwendung Serverberechtigungen und Zugriffsrechte.
2. Hinzufügen der Server des VoIP-Anbieters zur Sicherer Zone. Wenn Sie die IP-Adressen dieser Server nicht kennen, wenden Sie sich an den Kundendienst Ihres VoIP-Anbieters.

Verwenden von Web Conferencing

Wenn beim Ausführen eines Web Conferencing-Programms wie Microsoft NetMeeting Probleme auftreten, gehen Sie wie folgt vor:

1. Fügen Sie die Domäne oder IP-Adresse, zu der Sie eine Verbindung herstellen, der Sicherer Zone hinzu. Siehe **Hinzufügen zur Sicherer Zone** auf Seite [87](#).
2. Deaktivieren Sie die Option des Web Conferencing-Programms für die Freigabe des Remote-Desktops.

Full Disk Encryption

Full Disk Encryption ist eine Richtlinie-basierte Softwarelösung für die Unternehmenssicherheit. Full Disk Encryption gewährleistet mit einer Kombination aus Startschutz, Vorstart-Authentifizierung und starker Verschlüsselung, dass nur autorisierten Benutzern Zugriff auf die Daten auf Desktop- und Laptop-PCs gewährt wird.

Full Disk Encryption wird im gesamten Netzwerk bereitgestellt und verwaltet. Da die Verschlüsselung sowohl automatisch als auch transparent ist, wird die Sicherheit ohne besonderen Aufwand seitens der Benutzer durchgesetzt.

Inhalt dieses Abschnitts

Authentifizierung bei Full Disk Encryption	115
Ausschließen einer Computermanipulierung	116
Erstmalige Authentifizierung	116
Optionale Full Disk Encryption-Funktionen	121
Verwenden des Full Disk Encryption-Bildschirms	126

Authentifizierung bei Full Disk Encryption

In diesem Abschnitt wird behandelt, wie Sie ein festes Kennwort, ein dynamisches Token oder ein Smartcard-/USB-Token verwenden, um sich für den Zugriff auf Ihren mit Full Disk Encryption geschützten Computer zu authentifizieren.

Wenn ein Benutzer authentifiziert ist, bedeutet dies, dass Full Disk Encryption diesen Benutzer als eine Person bestätigt hat, die zur Verwendung eines bestimmten Computers autorisiert ist. Wenn Sie einen durch Full Disk Encryption geschützten Computer einschalten oder neu starten, wird das Dialogfeld Benutzerkonto identifizieren geöffnet.

Geben Sie einen gültigen Namen und ein gültiges Kennwort für das Benutzerkonto ein. Full Disk Encryption überprüft, ob Sie für den Zugriff auf den Computer autorisiert sind, und gibt den Computer gegebenenfalls zum Hochfahren frei.

Ausschließen einer Computermanipulierung

Wenn Sie den Rechner nicht selbst gestartet haben, sollten Sie vor Ihrer Authentifizierung den Computer stets durch Drücken von **STRG+ALT+ENTF** neu starten. Damit stellen Sie sicher, dass Ihr Computer nicht manipuliert wurde und Name und Kennwort Ihres Benutzerkontos nicht missbraucht werden können.

Erstmalige Authentifizierung

Im folgenden Abschnitt wird beschrieben, wie Sie als neuer Benutzer auf einen durch Full Disk Encryption geschützten Computer zugreifen.

Gehen wir davon aus, dass Ihr Administrator ein temporäres Benutzerkonto und Kennwort für Sie konfiguriert hat. In diesem Fall müssen Sie den temporären Namen und das temporäre Kennwort für Ihr Benutzerkonto verwenden, wenn Sie sich das erste Mal bei Full Disk Encryption authentifizieren.

Nach erfolgreicher Eingabe dieses Namens bzw. Kennworts für Ihr Benutzerkonto, fordert Sie Full Disk Encryption dazu auf, einen persönlichen (neuen) Namen für das Benutzerkonto und ein festes Kennwort einzugeben (oder ein dynamisches Token bzw. eine Smartcard für die Authentifizierung zu verwenden). Diese Anmeldeinformationen ersetzen in Zukunft den temporären Namen und das temporäre Kennwort des Benutzerkontos. Informationen zu Ihrem Benutzernamen und den Kennwortanforderungen erhalten Sie von Ihrem Administrator.

Statt eines temporären Benutzerkontos hat Ihr Administrator eventuell Ihr persönliches Benutzerkonto und Kennwort oder ein dynamisches Token bzw. eine Smartcard für Ihre Authentifizierung konfiguriert. Der Administrator teilt Ihnen mit, wie Sie sich das erste Mal authentifizieren.

Verwenden eines festen Kennworts

Ein festes Kennwort ist eine private Zeichenfolge, die nur Sie und Full Disk Encryption kennen und die Sie bei jedem Zugriff auf den Computer verwenden.

Ihr Full Disk Encryption-Administrator teilt Ihnen mit, welchen Namen und welches Kennwort Sie für Ihr Benutzerkonto beim ersten Zugriff auf einen durch Full Disk Encryption geschützten Computer einsetzen.

So authentifizieren Sie sich mit einem festen Kennwort:

1. Starten Sie Ihren durch Full Disk Encryption geschützten Computer.

Das Dialogfeld **Benutzerkonto identifizieren** wird geöffnet.



Hinweis – Wenn Sie den Computer nicht selbst gestartet haben, sollten Sie durch Drücken von STRG+ALT+ENTF sicherstellen, dass Ihr Computer nicht manipuliert wurde. Der Computer wird dann neu gestartet, und Full Disk Encryption zeigt wieder das Dialogfeld **Benutzerkonto identifizieren** an.

2. Geben Sie folgende Informationen an:
 - Geben Sie in das Feld **Name des Benutzerkontos** den Namen ein, den Sie vom Administrator für Ihr Benutzerkonto erhalten haben.
 - Geben Sie in das Feld **Kennwort** das Kennwort ein, das Sie vom Administrator erhalten haben. Das Kennwort wird während der Eingabe durch Sternchen (*) dargestellt und damit unkenntlich gemacht.
3. Klicken Sie auf **OK**.
4. Falls der Administrator Ihr normales Benutzerkonto statt eines temporären Kontos konfiguriert hat, klicken Sie auf **Fortfahren**. Sie sind nun authentifiziert, und Full Disk Encryption erlaubt den Start von Windows.

Wenn Ihr Administrator ein temporäres Benutzerkonto für Sie erstellt hat, zeigt Full Disk Encryption die folgende Meldung an:

Bevor Sie fortfahren, müssen Sie den temporären Namen für das Benutzerkonto in Ihren regulären Namen für das Benutzerkonto ändern und ein neues Kennwort festlegen. Der korrekte Name für Ihr Benutzerkonto wird möglicherweise bereits im nächsten Fenster angezeigt. Wenn dieser korrekt ist, brauchen Sie nur ein neues Kennwort festzulegen.

5. Klicken Sie auf **OK**, um das Meldungsfeld zu schließen.

Sie geben nun Ihren persönlichen (neuen) Namen und ein festes Kennwort für Ihr Benutzerkonto ein. Diese Anmeldeinformationen ersetzen in Zukunft den temporären Namen und das temporäre Kennwort, das bzw. den Sie gerade für das Benutzerkonto verwendet haben.

Das Dialogfeld für temporäre Benutzer wird geöffnet.

6. Geben Sie Ihren persönlichen Namen für das Benutzerkonto ein, und klicken Sie auf **OK**.

Das Dialogfeld **Neues Kennwort festlegen** wird geöffnet.

7. Geben Sie das feste Kennwort ein, das Sie verwenden möchten, und bestätigen Sie es. Klicken Sie dann auf OK.

Full Disk Encryption bestätigt, dass Sie zum ersten Mal erfolgreich mithilfe Ihrer Full Disk Encryption-Anmeldeinformationen auf den Computer zugegriffen haben.

8. Klicken Sie auf **Fortfahren**, um das Dialogfeld zu schließen.

Full Disk Encryption erlaubt nun das Starten von Windows.

Verwenden eines dynamischen Tokens

Ein dynamisches Token ist ein Kennwort, das Sie mithilfe eines Kennwort-Tokens immer dann generieren, wenn Sie von Full Disk Encryption authentifiziert werden möchten.

Ihr Full Disk Encryption-Administrator stellt Ihnen ein dynamisches Token, Informationen zum Umgang damit und einen Benutzernamen zur Verfügung.

So authentifizieren Sie sich mit einem dynamischen Token:

1. Starten Sie Ihren durch Full Disk Encryption geschützten Computer.

Das Dialogfeld **Benutzerkonto identifizieren** wird geöffnet.



Hinweis – Wenn Sie den Computer nicht selbst gestartet haben, sollten Sie durch Drücken von **STRG+ALT+ENTF** sicherstellen, dass Ihr Computer nicht manipuliert wurde. Der Computer wird dann neu gestartet, und Full Disk Encryption zeigt wieder das Dialogfeld **Benutzerkonto identifizieren** an.

2. Geben Sie in das Feld **Name des Benutzerkontos** den Benutzernamen ein, den Sie von Ihrem Administrator erhalten haben. Drücken Sie dann **TAB**.

Full Disk Encryption erkennt, dass Sie sich mit einem dynamischen Token authentifizieren möchten, und zeigt das Dialogfeld **Benutzerkonto identifizieren** an.

3. Geben Sie im dynamischen Token die Full Disk Encryption-Rückfrage ein, um eine Antwort zu generieren.
4. Geben Sie die Antwort in das Feld **Antwort** ein, und klicken Sie auf **OK**.

Full Disk Encryption bestätigt, dass Sie zum ersten Mal erfolgreich mithilfe Ihrer Full Disk Encryption-Anmeldeinformationen auf den Computer zugegriffen haben.

5. Klicken Sie auf **Fortfahren**, um das Dialogfeld zu schließen.

Full Disk Encryption erlaubt nun das Starten von Windows.

Verwenden einer Smartcard/eines USB-Tokens

Auf Smartcards und USB-Token sind Zertifikate gespeichert, die durch PIN-Codes geschützt sind. Zur Authentifizierung durch Full Disk Encryption müssen Sie die Karte oder den Token an den Computer anschließen und eine gültige PIN für die Karte bzw. den Token eingeben.

Ihr Full Disk Encryption-Administrator stellt Ihnen Ihre Smartcard/Ihr USB-Token, die Informationen zum Umgang damit und gegebenenfalls einen temporären Benutzernamen und ein temporäres Kennwort für den ersten Zugriff auf den durch Full Disk Encryption geschützten Computer zur Verfügung.

Stellen Sie sicher, dass Ihre Smartcard/Ihr USB-Token an den Computer angeschlossen ist, bevor Sie den Authentifizierungsvorgang beginnen.

So authentifizieren Sie sich mit einer Smartcard bzw. einem USB-Token:

1. Schließen Sie Ihre Smartcard/Ihr USB-Token an Ihren durch Full Disk Encryption geschützten Computer an.
2. Starten Sie den Computer.

Das Dialogfeld **Benutzerkonto identifizieren** wird geöffnet.



Hinweis – Wenn Sie den Computer nicht selbst gestartet haben, sollten Sie durch Drücken von STRG+ALT+ENTF sicherstellen, dass Ihr Computer nicht manipuliert wurde. Der Computer wird dann neu gestartet, und Full Disk Encryption zeigt wieder das Dialogfeld **Benutzerkonto identifizieren** an.

3. Geben Sie folgende Informationen an:
 - Geben Sie in das Feld **Name des Benutzerkontos** den Namen ein, den Sie vom Administrator für Ihr Benutzerkonto erhalten haben.
 - Geben Sie in das Feld **Kennwort** das Kennwort ein, das Sie vom Administrator erhalten haben. Das Kennwort wird während der Eingabe durch Sternchen (*) dargestellt und damit unkenntlich gemacht.
4. Klicken Sie auf OK.

Falls der Administrator Ihr normales Benutzerkonto statt eines temporären Kontos konfiguriert hat, überspringen Sie die nächsten beiden Schritte.

Wenn Ihr Administrator ein temporäres Benutzerkonto für Sie erstellt hat, zeigt Full Disk Encryption die folgende Meldung an:

Bevor Sie fortfahren, müssen Sie den temporären Namen für das Benutzerkonto in Ihren regulären Namen für das Benutzerkonto ändern und ein neues Kennwort festlegen. Der korrekte Name für Ihr Benutzerkonto wird möglicherweise bereits im nächsten Fenster angezeigt. Wenn dieser korrekt ist, brauchen Sie nur ein neues Kennwort festzulegen.

5. Klicken Sie auf OK, um das Meldungsfeld zu schließen.

Das Dialogfeld für temporäre Benutzer wird geöffnet.

6. Geben Sie Ihren neuen Namen für das Benutzerkonto ein, und klicken Sie auf OK.

Full Disk Encryption erkennt, dass Sie über ein Benutzerkonto verfügen, das die Authentifizierung über eine Smartcard durchführt. FDE bestätigt, dass Sie sich zum ersten Mal mit dem neuen Namen für das Benutzerkonto angemeldet haben. Das Dialogfeld **Anmeldung erfolgreich** wird geöffnet.

7. Klicken Sie auf Fortfahren.

Nachdem Windows geladen wurde, wird das Dialogfeld **Anmeldeinformationen ändern** angezeigt.

8. Wählen Sie das zu verwendende Zertifikat aus, und klicken Sie auf OK.



Wichtig – Ändern Sie NICHT das Zertifikat Privater Speicher. Wenn Sie dies tun, können Sie sich nach dem Neustart des Computers nicht authentifizieren.

Full Disk Encryption bestätigt, dass Ihr Benutzerzertifikat aktualisiert wurde.

9. Klicken Sie auf OK.

10. Starten Sie den Computer bei entsprechender Aufforderung neu.

Nach dem Neustart wird das Dialogfeld zur Token-Authentifizierung geöffnet.

11. Geben Sie Ihre PIN ein. Die PIN wird während der Eingabe durch Sternchen (*) dargestellt und damit unkenntlich gemacht.

12. Klicken Sie auf OK.



Hinweis – Ungeachtet der verwendeten Tastaturbelegung empfehlen wir, für Smartcard-PINs nur ASCII-Zeichen zu verwenden:

!"#\$%&'()*+,-./ 0123456789:;<=>?@

ABCDEFGHIJKLMNOPQRSTUVWXYZ

[] ^ _ ` abcdefghijklmnopqrstuvwxyz { } ~

Das Leerzeichen zählt ebenfalls zu den ASCII-Zeichen.

Full Disk Encryption kommuniziert mit der Smartcard und führt die Authentifizierung durch.

13. Klicken Sie auf OK.

Vorgehensweise bei einem vergessenen Kennwort

Falls Sie einmal Ihr Kennwort vergessen, können Sie von der Full Disk Encryption-Option Kennwortänderung Gebrauch machen.

So ändern Sie Ihr Kennwort:

1. Starten Sie Ihren durch Full Disk Encryption geschützten Computer. Das Dialogfeld **Benutzerkonto identifizieren** wird geöffnet.
2. Geben Sie den Namen Ihres Benutzerkontos ein, und wählen Sie **Remote-Hilfe** aus.

Das Dialogfeld **Anmeldung bei der Remote-Hilfe** wird geöffnet.

3. Wenden Sie sich an Ihren Full Disk Encryption-Administrator oder an Ihr Helpdesk, um eine schrittweise Anleitung zur Kennwortänderung zu erhalten.

Kein Zugriff auf den Token/die Smartcard

Wenn Sie keinen Zugriff auf Ihren dynamischen Token oder Ihre Smartcard haben, steht Ihnen die Full Disk Encryption-Option **Einmalige Anmeldung** zur Verfügung.

So verwenden Sie diese Option:

1. Starten Sie Ihren durch Full Disk Encryption geschützten Computer. Das Dialogfeld **Benutzerkonto identifizieren** wird geöffnet.
2. Geben Sie den Namen Ihres Benutzerkontos ein, und wählen Sie **Remote-Hilfe** aus.

Das Dialogfeld **Anmeldung bei der Remote-Hilfe** wird geöffnet.

3. Wählen Sie die Option **Einmalige Anmeldung** aus, um diese Funktion zu aktivieren. Wenden Sie sich an Ihren Full Disk Encryption-Administrator oder an Ihr Helpdesk, um eine schrittweise Anleitung zur einmaligen Anmeldung zu erhalten.

Optionale Full Disk Encryption-Funktionen

In diesem Abschnitt werden einige optionalen Funktionen beschrieben, die Ihr Administrator unter Umständen für Ihre Full Disk Encryption-Installation konfiguriert hat. So könnten Sie in Abhängigkeit von der Konfiguration in der Lage

sein, für die Anmeldung bei Windows und für die Authentifizierung bei Full Disk Encryption dasselbe Kennwort zu verwenden. Eventuell ist es auch gar nicht erforderlich, dass Sie Ihre Full Disk Encryption-Anmeldeinformationen eingeben.

Synchronisieren von Kennwörtern

Mithilfe der Kennwortsynchronisierung von Full Disk Encryption können Sie Windows- und Full Disk Encryption-Kennwörter miteinander abgleichen, sofern der Administrator die Kennwortsynchronisierung für Ihr Benutzerkonto aktiviert hat.

Abhängig von den Einstellungen, die Ihr Administrator konfiguriert hat, kann Ihr Kennwort anhand einer oder beider der folgenden Möglichkeiten synchronisiert werden:

- Authentifizierung bei Full Disk Encryption mit Windows-Kennwort
Wenn diese Synchronisierungsoption für Sie konfiguriert wurde, wird das Windows-Kennwort auch für die Vorstart-Authentifizierung von Full Disk Encryption verwendet. Nach der Synchronisierung wird bei Änderung des Windows-Kennworts das Full Disk Encryption-Kennwort automatisch auf das neue Windows-Kennwort eingestellt.
(In der Administratoranwendung heißt diese Einstellung **Windows-Kennwort mit Vorstart-Kennwort synchronisieren**.)
- Für Windows-Anmeldung das Full Disk Encryption-Kennwort verwenden
Wenn diese Synchronisierungsoption für Sie konfiguriert wurde, wird das Kennwort für die Vorstart-Authentifizierung von Full Disk Encryption auch für die Windows-Authentifizierung verwendet. Nach der Synchronisierung wird bei Änderung des Full Disk Encryption-Kennworts das Windows-Kennwort automatisch auf das neue Full Disk Encryption-Kennwort eingestellt.
(In der Administratoranwendung heißt diese Einstellung **Vorstart-Kennwort mit Windows-Kennwort synchronisieren**.)

Verwenden des Windows-Kennworts für Full Disk Encryption

Wenn die Richtlinie für Ihre Kennwortsynchronisierung so geändert wurde, dass Sie sich mit dem Windows-Kennwort bei Full Disk Encryption authentifizieren, werden die Kennwörter in folgenden Fällen synchronisiert:

- Änderung des Windows-Kennworts
oder
- Erste Anmeldung bei Windows nach der Änderung der Richtlinie

Sie werden zur Eingabe Ihres Full Disk Encryption-Kennworts aufgefordert, und dieses Kennwort wird dann mit dem Windows-Kennwort synchronisiert.

Nach der Synchronisierung der Kennwörter wird bei Änderung des Windows-Kennworts das Full Disk Encryption-Kennwort automatisch auf das neue Windows-Kennwort eingestellt.

So synchronisieren Sie das Full Disk Encryption-Kennwort mit dem Windows-Kennwort:

1. Wenn Sie Ihr Windows-Kennwort geändert haben oder sich bei Windows zum ersten Mal nach einer Änderung der Richtlinie anmelden, wird das Dialogfeld zur Kennwortsynchronisierung geöffnet.
2. Geben Sie Ihr Full Disk Encryption-Kennwort an, und klicken Sie auf OK.
Full Disk Encryption bestätigt die Änderung Ihres Kennworts.
Verwenden Sie von jetzt an Ihr Windows-Kennwort zur Authentifizierung bei Full Disk Encryption.

Verwenden des Full Disk Encryption-Kennworts für Windows

Wenn die Richtlinie für Ihre Kennwortsynchronisierung so geändert wurde, dass Sie sich mit dem Full Disk Encryption-Kennwort bei Windows anmelden, werden die Kennwörter in folgenden Fällen synchronisiert:

- Ändern Ihres Full Disk Encryption-Kennworts
Wenn Sie Ihr Full Disk Encryption-Kennwort ändern, werden Sie zur Eingabe Ihres Windows-Kennworts aufgefordert. Es wird dann mit Ihrem Full Disk Encryption-Kennwort synchronisiert.
- Erste Anmeldung bei Windows nach der Änderung der Richtlinie
Die Kennwörter werden automatisch synchronisiert.

Nach der Synchronisierung der Kennwörter wird bei Änderung des Full Disk Encryption-Kennworts das Windows-Kennwort automatisch auf das neue Full Disk Encryption-Kennwort eingestellt.

Single Sign-On und OneCheck Logon

In diesem Abschnitt wird beschrieben, wie Sie die Anmeldung mit Single Sign-On (SSO) oder mit OneCheck Logon durchführen.

- **Single Sign-On:** Die Funktion Single Sign-On (SSO) bietet Ihnen die Möglichkeit, sich bei Full Disk Encryption zu authentifizieren und anschließend

automatisch eine Authentifizierung und Anmeldung bei Windows durchzuführen.

- **OneCheck Logon:** Die Funktion OneCheck Logon ermöglicht Ihnen die Authentifizierung bei Full Disk Encryption und die automatische Authentifizierung und Anmeldung bei Windows, dem Endpoint Connect VPN und bei Media Encryption.



Hinweis – Ihr Full Disk Encryption-Administrator legt fest, ob Sie auf die Funktionen SSO und OneCheck Logon zugreifen können.

Erste Anmeldung nach Aktivierung von SSO oder OneCheck Logon

Nachdem der Administrator SSO oder OneCheck Logon für Ihr Full Disk Encryption-Benutzerkonto auf einem Computer aktiviert hat, muss Full Disk Encryption die Anmeldeinformationen für Ihr Konto lernen. Dies erfolgt bei der ersten Anmeldung nach Aktivierung von SSO oder OneCheck Logon. Dabei melden Sie sich wie gewohnt bei Windows an. Full Disk Encryption speichert dann Ihre Anmeldeinformationen sicher und verwendet sie bei nachfolgenden Anmeldungen, für die SSO oder OneCheck Logon aktiviert wurde.

Aufheben der Auswahl der SSO-Option

Ist die SSO-Option nicht ausgewählt (das Kontrollkästchen SSO aktiv ist nicht aktiviert), werden keine Anmeldeinformationen an Windows übergeben. Damit haben Sie die Möglichkeit, ein anderes Windows-Benutzerkonto zu verwenden.

Bei der Deaktivierung von SSO werden keine Windows-Anmeldeinformationen aufgezeichnet oder verwendet. Die Kette ist somit unterbrochen. Wenn SSO wieder aktiviert wird, müssen die vorherigen Anmeldeinformationen erneut angegeben werden, damit SSO wieder funktionsfähig ist.

SSO, OneCheck Logon und Kennwortänderungen

Das Windows-Kennwort muss in regelmäßigen Abständen geändert werden. In diesem Fall übernimmt Full Disk Encryption die Änderungen aus dem Dialogfeld **Kennwort ändern**. Wenn das Dialogfeld **Kennwort ändern** geöffnet wird, zeichnet Full Disk Encryption die Eingabe in das Feld für das neue Kennwort auf. Beim nächsten Neustart des Computers funktionieren SSO oder OneCheck Logon wie immer, da das neue Kennwort bereits gespeichert wurde.

Anmelden bei aktivierter SSO- oder OneCheck Logon-Funktion

Ist SSO oder OneCheck Logon aktiviert, erfolgt die Anmeldung ähnlich wie die Anmeldung ohne diese Funktionen. Sie dürfen nur nicht vergessen, das Kontrollkästchen SSO aktiv zu aktivieren. Für OneCheck Logon wird dasselbe Dialogfeld verwendet.

So melden Sie sich mit aktiviertem SSO an:

1. Authentifizieren Sie sich wie immer im Dialogfeld **Benutzerkonto identifizieren**.
2. Stellen Sie sicher, dass das Kontrollkästchen SSO aktiv aktiviert ist, und klicken Sie auf OK.

Ihr Computer wird gestartet, und Sie werden mit SSO automatisch bei Windows angemeldet. Mit OneCheck Logon werden Sie automatisch bei Windows und entweder beim Endpoint Connect VPN, bei Media Encryption oder bei beidem angemeldet.



Hinweis – Wenn Ihr Administrator die Funktion SSO aktiv aktiviert hat, können Sie diese Option deaktivieren und SSO nicht verwenden.

Integrierte Windows-Anmeldung

Wenn Ihr Administrator die Funktion **Integrierte Windows-Anmeldung (WIL)** ausgewählt hat, werden Sie ohne Eingabe Ihrer Full Disk Encryption-Anmeldeinformationen normal bei Windows angemeldet.

In Abhängigkeit von den Einstellungen, die Ihr Full Disk Encryption-Administrator konfiguriert hat, können Sie Windows unter Umständen nicht im abgesicherten Modus starten.

Ferner müssen Sie sich in folgenden Fällen selbst bei Full Disk Encryption authentifizieren:

- Ihr WIL-aktivierter Computer wurde aus dem Netzwerk entfernt.
- Ihrem WIL-aktivierten Computer wurden Hardwaregeräte hinzugefügt, oder am Festplattenlaufwerk wurden unbefugte Änderungen vorgenommen.
- Das Festplattenlaufwerk wurde zu einem anderen Computer transferiert.
- Die zulässige Anzahl fehlgeschlagener Windows-Anmeldeversuche wurde überschritten.

Wenn das System erkennt, dass einer dieser Fälle vorliegt, wird WIL automatisch deaktiviert. Der Computer wird dann neu gestartet, und Sie müssen sich bei Full Disk Encryption authentifizieren, bevor das Betriebssystem geladen wird.

Verwenden des Full Disk Encryption-Bildschirms

In diesem Abschnitt wird die Verwendung des Bildschirms Full Disk Encryption von Endpoint Security Client erklärt, auf den Sie zugreifen, nachdem Sie sich bei Full Disk Encryption authentifiziert und Zugriff auf das Betriebssystem erlangt haben. Im Bildschirm Full Disk Encryption können Sie Folgendes tun:

- Status- und Verschlüsselungsinformationen anzeigen
- Ihre Full Disk Encryption-Benutzeranmeldeinformationen ändern
- Die Sprache der Benutzeroberfläche des Full Disk Encryption Clients ändern

Anzeigen von Status- und Verschlüsselungsinformationen

Sie können die Statusinformationen Ihrer Full Disk Encryption-Installation im Bildschirm Full Disk Encryption anzeigen.

So zeigen Sie Statusinformationen an:

Wählen Sie Full Disk Encryption | Grundeinstellungen.

Full Disk Encryption-Statusinformationen

Im Bildschirm Full Disk Encryption | Grundeinstellungen werden folgende Statusinformationen angezeigt.

Statusfeld	Erläuterung
Lokal installierte Version	Die derzeit auf dem jeweiligen Computer installierte Version von Full Disk Encryption.
Benutzerkonto vorladen	Der Name des Benutzerkontos, das vor dem Start authentifiziert wurde.
FDEMC-Benutzerkonto	Der Name des Benutzerkontos, das derzeit bei Full Disk Encryption Management Console (FDEMC) angemeldet ist (wenn zutreffend).
MI-Modus	Gibt an, ob diese Installation von Full Disk Encryption im MI-Modus ausgeführt wird oder nicht. Mögliche Werte: Ja oder Nein.
Integrierte Windows-Anmeldung	Der Wert, der derzeit für die Einstellung Integrierte Windows-Anmeldung festgelegt ist. Mögliche Werte: Aktiviert oder Deaktiviert.

Letzte Wiederherstellungsaktualisierung	Erstellungsdatum und -uhrzeit der aktuellsten Wiederherstellungsdatei.
Letzte Bereitstellung der Wiederherstellungsdatei	Datum und Uhrzeit des letzten Kopiervorgangs einer Wiederherstellungsdatei zum Zielverzeichnis. Das Zielverzeichnis ist das Verzeichnis, das unter dem Wiederherstellungspfad in den Installationseinstellungen unter Systemeinstellungen angegeben wurde.
Letzte Aktualisierung der Protokolldatei	Datum und Uhrzeit der letzten Aktualisierung der Protokolldatei durch Full Disk Encryption.
Letzte Bereitstellung der Protokolldatei	Datum und Uhrzeit des letzten Full Disk Encryption-Schreibvorgangs in die Protokolldatei. Der Dateiname der logischen Protokolldatei ist mit dem Namen des Rechners identisch. Die logische Protokolldatei wird in dem oder den Verzeichnis(sen) abgelegt, die bzw. das unter Zentrale(n) Protokollpfad(e) festlegen angegeben wurde(n) (Installationseinstellungen unter Systemeinstellungen).
Letzte lokale Bearbeitung	Datum und Uhrzeit der letzten Änderung an einer lokalen Einstellung. Umfasst auch den Gruppen- und Benutzerkontonamen des Benutzers, der die Änderung vorgenommen hat.
Letzte Profilaktualisierung	Datum und Uhrzeit des letzten Downloads einer Profilaktualisierung sowie der Pfad, einschließlich Profilname, von dem die Profilaktualisierung heruntergeladen wurde.
Ablaufdatum für Lizenz	Datum, an dem die Lizenz abläuft. Das Ablaufdatum wird nur für Testversionen des Produkts verwendet.
Lizenzaktivierung	Status der Full Disk Encryption-Lizenz.

Informationen zur Full Disk Encryption-Lizenzaktivierung

Die Lizenzaktivierung kann über folgende Stati verfügen:

- **Lizenz aktiviert:** Normalerweise wird die Lizenz automatisch auf dem für Ihre Installation verwendeten Lizenzserver aktiviert.
- **Lizenz nicht aktiviert:** Wenn Ihre Lizenz aus irgendwelchen Gründen nicht aktiviert ist, fordert Sie Full Disk Encryption in Dialogfeldern dazu auf, die

Lizenz auf dem Lizenzserver zu aktivieren. Wenn dies der Fall ist, achten Sie darauf, dass Sie online sind. Ist dies der Fall, werden die Informationen automatisch an den Lizenzserver übertragen. Sollte Full Disk Encryption weiterhin Dialogfelder mit Aufforderungen anzeigen (auch wenn Sie online sind), wenden Sie sich an Ihr Helpdesk.

- **Aktivierung deaktiviert:** Wenn Sie eine veraltete Lizenz verwenden, die nicht auf dem Lizenzserver registriert werden kann, wird die Lizenzaktivierung deaktiviert.

Verschlüsselungsinformationen

Die folgenden Verschlüsselungsinformationen werden für die einzelnen Volumes angezeigt:

Statusfeld	Erläuterung
nn % verschlüsselt	Zeigt in Prozent an, wie weit die Verschlüsselung fortgeschritten ist.
Vollständig verschlüsselt	Zeigt an, dass das Volume vollständig verschlüsselt wurde.
nn % entschlüsselt	Zeigt in Prozent an, wie weit die Entschlüsselung fortgeschritten ist.
Nicht verschlüsselt	Zeigt an, dass das Volume nicht verschlüsselt ist.
Fehler	Während der Ver- oder Entschlüsselung ist ein Fehler aufgetreten.



Hinweis – Wenn ein Volume nicht verschlüsselt ist oder dafür kein Startschutz vorliegt, wird es im Feld mit den Verschlüsselungsinformationen nicht aufgeführt.

Ändern der Anmeldeinformationen für die Authentifizierung

Im Bildschirm Full Disk Encryption können Sie Folgendes ausführen:

- Das Kennwort ändern, sofern Sie sich mit einem festen Kennwort authentifizieren.
- Die aktuelle Authentifizierungsmethode (Anmeldemethode) ändern: festes Kennwort, dynamischer Token, Smartcard. Die Authentifizierungsmethoden, auf die Sie umstellen können, sind im Dialogfeld **Anmeldeinformationen ändern**

unter **Anmeldemethode** aktiv. Die anderen sind abgeblendet, da sie nicht zur Verfügung stehen.

So ändern Sie die Anmeldeinformationen:

1. Öffnen Sie **Full Disk Encryption | Erweitert**.
2. Klicken Sie auf **Ändern**.

Das Dialogfeld für die Full Disk Encryption-Authentifizierung wird geöffnet.

3. Führen Sie im Dialogfeld für die Full Disk Encryption-Authentifizierung die Authentifizierung durch. Wenn Sie sich über eine Smartcard authentifizieren, wählen Sie **Eingelegte Smartcard verwenden** aus.

Falls Sie für die Authentifizierung Remote-Hilfe benötigen, wenden Sie sich an den für Remote-Hilfe zuständigen Administrator. Er wird Sie durch den Remote-Hilfevorgang leiten.

Nach der erfolgreichen Authentifizierung wird das Dialogfeld **Anmeldeinformationen ändern** angezeigt.

Im Dialogfeld **Anmeldeinformationen ändern** werden die Anmeldemethoden angezeigt, die Ihnen zur Verfügung stehen. Dazu gehören:

- **Festes Kennwort:** Geben Sie ein neues Kennwort ein, und bestätigen Sie dieses, falls Sie sich mit einem festen Kennwort authentifizieren. Wenn das Kontrollkästchen **Eingabe verbergen** aktiviert ist, werden die eingegebenen Zeichen als Sternchen (*) dargestellt und damit unkenntlich gemacht. Andernfalls werden die tatsächlich eingegebenen Zeichen angezeigt. Das Dialogfeld enthält Anleitungen zur Gültigkeit des eingegebenen Kennworts.
 - **Dynamisches Token:** Geben Sie die erforderlichen Informationen ein.
 - **Smartcard:** Geben Sie die erforderlichen Informationen ein.
4. Wählen Sie unter den verfügbaren Anmeldemethoden eine Methode aus, auf die Sie umstellen möchten.
 5. Klicken Sie auf **OK**.

Ändern der Sprache für die Benutzeroberfläche

Sie können die Sprache ändern, die in der Vorstart-Oberfläche, der Taskleiste, dem Wiederherstellungsdienstprogramm und der Single Sign-On-Oberfläche (sofern aktiviert) des Full Disk Encryption Clients verwendet wird.

So ändern Sie die verwendete Sprache:

1. Öffnen Sie Full Disk Encryption | Erweitert.
2. Wählen Sie aus dem Dropdown-Menü **Sprache auswählen** die zu verwendende Sprache aus.
3. Schließen Sie den Endpoint Security Client. Wenn Sie Full Disk Encryption das nächste Mal starten, wird im Dialogfeld der Vorstart-Umgebung die ausgewählte Sprache verwendet.

Unterstützte Sprachen

Die folgenden Sprachen werden in der Vorstart-Umgebung von Full Disk Encryption unterstützt:

BR	Portugiesisch (Brasilien)
CA	Französisch (Kanada)
CN	Chinesisch (vereinfacht)
CZ	Tschechisch
DE	Deutsch
ES	Spanisch
FR	Französisch
HU	Ungarisch
IT	Italienisch
JP	Japanisch
KO	Koreanisch
PL	Polnisch
PT	Portugiesisch
RU	Russisch
TH	Thailändisch
TW	Chinesisch (traditionell)
US	Englisch



Hinweis – Sie können auch die Sprache des Betriebssystems auswählen, die im Dropdown-Menü aufgeführt ist. Falls **Betriebssystem** ausgewählt ist und die Sprache des Betriebssystems nicht eine der unterstützten Sprachen ist, wird US-amerikanisches Englisch angezeigt.

Ausweichsprachen

Falls die Sprache des Betriebssystems eine nicht unterstützte Variante einer der unterstützten Sprachen ist, beispielsweise Französisch (Kanada) oder Chinesisch (Singapur), wird die in der folgenden Tabelle aufgeführte Sprachvariante aus Ausweichsprache verwendet:

ID	Ausgewählte Sprache	Ausweichsprache	ID
0x0C04	Chinesisch (Hong Kong SAR)	Chinesisch (traditionell)	0x7C04
0x1404	Chinesisch (Macau SAR)	Chinesisch (traditionell)	0x7C04
0x0804	Chinesisch (Volksrepublik China)	Chinesisch (vereinfacht)	0x0004
0x0004	Chinesisch (vereinfacht)	Chinesisch (vereinfacht)	0x0004
0x1004	Chinesisch (Singapur)	Chinesisch (vereinfacht)	0x0004
0x0404	Chinesisch (Taiwan)	Chinesisch (traditionell)	0x7C04
0x7C04	Chinesisch (traditionell)	Chinesisch (traditionell)	0x7C04
0x0009	Englisch	Englisch (USA)	0x0409
0x0C09	Englisch (Australien)	Englisch (USA)	0x0409
0x2809	Englisch (Belize)	Englisch (USA)	0x0409
0x1009	Englisch (Kanada)	Englisch (USA)	0x0409
0x2409	Englisch (Karibik)	Englisch (USA)	0x0409
0x1809	Englisch (Irland)	Englisch (USA)	0x0409
0x2009	Englisch (Jamaika)	Englisch (USA)	0x0409
0x1409	Englisch (Neuseeland)	Englisch (USA)	0x0409

ID	Ausgewählte Sprache	Ausweichsprache	ID
0x3409	Englisch (Republik der Philippinen)	Englisch (USA)	0x0409
0x1C09	Englisch (Südafrika)	Englisch (USA)	0x0409
0x2C09	Englisch (Trinidad und Tobago)	Englisch (USA)	0x0409
0x0809	Englisch (Vereinigtes Königreich)	Englisch (Vereinigtes Königreich)	0x0809
0x0409	Englisch (USA)	Englisch (USA)	0x0409
0x3009	Englisch (Simbabwe)	Englisch (USA)	0x0409
0x000C	Französisch	Französisch (Frankreich)	0x040C
0x080C	Französisch (Belgien)	Französisch (Frankreich)	0x040C
0x0C0C	Französisch (Kanada)	Französisch (Frankreich)	0x040C
0x040C	Französisch (Frankreich)	Französisch (Frankreich)	0x040C
0x140C	Französisch (Luxemburg)	Französisch (Frankreich)	0x040C
0x180C	Französisch (Fürstentum Monaco)	Französisch (Frankreich)	0x040C
0x100C	Französisch (Schweiz)	Französisch (Frankreich)	0x040C
0x0007	Deutsch	Deutsch (Deutschland)	0x0407
0x0C07	Deutsch (Österreich)	Deutsch (Deutschland)	0x0407
0x0407	Deutsch (Deutschland)	Deutsch (Deutschland)	0x0407
0x1407	Deutsch (Liechtenstein)	Deutsch (Deutschland)	0x0407
0x1007	Deutsch (Luxemburg)	Deutsch (Deutschland)	0x0407
0x0807	Deutsch (Schweiz)	Deutsch	0x0407

ID	Ausgewählte Sprache	Ausweichsprache	ID
		(Deutschland)	
0x0010	Italienisch	Italienisch (Italien)	0x0410
0x0410	Italienisch (Italien)	Italienisch (Italien)	0x0410
0x810	Italienisch (Schweiz)	Italienisch (Italien)	0x0410
0x0011	Japanisch	Japanisch (Japan)	0x0411
0x0411	Japanisch (Japan)	Japanisch (Japan)	0x0411
0x0019	Russisch	Russisch (Russland)	0x0419
0x0419	Russisch (Russland)	Russisch (Russland)	0x0419
0x000A	Spanisch	Spanisch (Spanien)	0x0C0A
0x2C0A	Spanisch (Argentinien)	Spanisch (Spanien)	0x0C0A
0x400A	Spanisch (Bolivien)	Spanisch (Spanien)	0x0C0A
0x340A	Spanisch (Chile)	Spanisch (Spanien)	0x0C0A
0x240A	Spanisch (Kolumbien)	Spanisch (Spanien)	0x0C0A
0x140A	Spanisch (Costa Rica)	Spanisch (Spanien)	0x0C0A
0x1C0A	Spanisch (Dominikanische Republik)	Spanisch (Spanien)	0x0C0A
0x300A	Spanisch (Ecuador)	Spanisch (Spanien)	0x0C0A
0x440A	Spanisch (El Salvador)	Spanisch (Spanien)	0x0C0A
0x100A	Spanisch (Guatemala)	Spanisch (Spanien)	0x0C0A
0x480A	Spanisch (Honduras)	Spanisch (Spanien)	0x0C0A
0x080A	Spanisch (Mexiko)	Spanisch (Spanien)	0x0C0A
0x4C0A	Spanisch (Nicaragua)	Spanisch (Spanien)	0x0C0A
0x180A	Spanisch (Panama)	Spanisch (Spanien)	0x0C0A
0x3C0A	Spanisch (Paraguay)	Spanisch (Spanien)	0x0C0A
0x280A	Spanisch (Peru)	Spanisch (Spanien)	0x0C0A
0x500A	Spanisch (Puerto Rico)	Spanisch (Spanien)	0x0C0A
0x0C0A	Spanisch (Spanien)	Spanisch (Spanien)	0x0C0A
0x380A	Spanisch (Uruguay)	Spanisch (Spanien)	0x0C0A
0x200A	Spanisch (Venezuela)	Spanisch (Spanien)	0x0C0A

In der Vorstart-Umgebung unterstützte Zeichen

Die folgenden Zeichen werden in der Vorstart-Umgebung von Full Disk Encryption unterstützt:

[illegible]

Media Encryption

Check Point Media Encryption ist eine einzigartige Lösung, die einen richtliniengesteuerten Mechanismus zum Schutz von Unternehmensinformationen und zur Gewährleistung der Datenintegrität bereitstellt. Das Produkt umfasst die unten aufgeführten Funktionen, die vom Systemadministrator festgelegt werden.

Media Encryption ist ein integraler Bestandteil von Check Point Endpoint Security Client. Endpoint Security Client kombiniert Firewall, Netzwerkzugriffskontrolle, Program Control, Anti-Malware-Software, Datensicherheit und Remote-Zugriffsschutz in einer einheitlichen Anwendung mit einer gemeinsamen Benutzeroberfläche.

Inhalt dieses Abschnitts

Funktionen	135
Verwenden des EPM Clients	139
Verwenden des Managers für Wechselmedien	146
Verwenden des Gerätemanagers	147
Verwenden von Program Security Guard	148
Bereich "Wartung"	148

Funktionen

So zeigen Sie die Einstellungen für Media Encryption an und bearbeiten diese:

1. Klicken Sie mit der rechten Maustaste auf das Symbol in der Taskleiste, und wählen Sie **Einstellungen**.

Der Check Point Endpoint Security Client wird geöffnet.

2. Klicken Sie in der Liste auf **Media Encryption**.

Das Hauptfenster von Media Encryption wird geöffnet. Von Ihrem Systemadministrator deaktivierte Funktionen werden grau angezeigt.

Encryption Richtlinie Manager

Der optionale Encryption Richtlinie Manager (EPM) ermöglicht Benutzern, Daten auf Wechselmedien, die an ihren Endpunkt-Computern angeschlossen sind, zu verschlüsseln und den Zugriff darauf zu steuern. Wenn Sie Zugriff auf Wechselmediengeräte gewähren, besteht die größte Gefahr darin, dass sensible oder vertrauliche Daten in die falschen Hände geraten. Mit Encryption Richtlinie Manager können Sie dafür sorgen, dass diese Daten nur autorisierten Personen auf autorisierten Systemen zugänglich sind.

Encryption Richtlinie Manager ermöglicht die transparente Verschlüsselung von Wechselmediengeräten. Dazu gehört die Verschlüsselung von CDs oder DVDs unter Verwendung der in Windows integrierten Software auf den von Media Encryption geschützten Arbeitsplatzrechnern. Abhängig davon, wie Media Encryption von Ihrem SystemAdministrator eingerichtet wurde, können Sie auch dann auf verschlüsselten Geräten gespeicherte Daten zugreifen, wenn Sie offline sind. Sie können auch auf verschlüsselte Geräte auf Computern zugreifen, auf denen Media Encryption nicht installiert ist, sofern das Medium für diesen Zugriff verschlüsselt wurde und Sie das Kennwort für das Gerät besitzen.

Manager für Wechselmedien

Der Manager für Wechselmedien steuert den Zugriff auf Wechselmedien und Geräte wie die Folgenden: Diskettenlaufwerke, PDAs, Flash-Speicher, Digitalkameras, externe Festplatten (FAT-formatiert) usw. Er steuert den Gerätezugriff für alle verfügbaren Ports, einschließlich USB und Firewire. CD- und DVD-Laufwerke werden durch den Gerätemanager geschützt. Weitere Informationen finden Sie im Abschnitt **Gerätemanager** auf Seite [137](#).

Alle Wechselmedien (außer CDs/DVDs und NTFS-formatierte externe Festplatten) müssen autorisiert werden, bevor der Zugriff gewährt wird. Beim Autorisieren von Wechselmedien muss eine digitale Signatur auf dem Medium selbst gespeichert werden. Wenn diese Signatur nicht vorhanden ist, kann auf Wechselmedien von einem geschützten Endpunkt-Computer nicht zugegriffen werden.

Ihr SystemAdministrator steuert die Autorisierung durch Definieren von Regeln für den Manager für Wechselmedien in einer Media Encryption-Richtlinie, die auf Ihrem Computer installiert ist. Regeln definieren Zugriffsrechte für die einzelnen

Arten von Wechselmedien, einschließlich Voraussetzungen wie Virenprüfung und Datenautorisierung.

Die digitale Signatur wird automatisch aktualisiert, wenn Sie Daten von einem oder auf ein Gerät bewegen und sich innerhalb der geschützten Umgebung befinden. Wenn Änderungen des Mediums außerhalb des Unternehmens zulässig sind, muss das Gerät erneut autorisiert werden, d. h. Sie müssen ein Kennwort eingeben, und Media Encryption muss das Gerät erneut autorisieren, bevor es wieder innerhalb der geschützten Umgebung verwendet werden kann.

Media Encryption stellt sicher, dass alle Geräte virenfrei sind und unterbindet das nicht autorisierte Verschlüsseln und Entschlüsseln von Daten. Abhängig von der Konfiguration kann Media Encryption Ihnen den Zugriff auf nicht autorisierte Hot-Swap- und Plug-and-Play-Geräte verweigern.

Gerätemanager

Der Media Encryption-Gerätemanager steuert den Zugriff auf Geräte, die mit den verschiedenen Anschlüssen Ihres Computers verbunden sind. Ihr SystemAdministrator kann Regeln für die folgenden Anschlüsse aufstellen: IrDA, COM, USB, Firewire und LPT. Diese Regeln legen fest, ob Sie Lesezugriff, Lese-/Schreibzugriff und/oder Ausführungszugriff für Wechselmedien besitzen, die an Ihren Computer angeschlossen sind, wie CD/DVD-Laufwerke, PDAs, Blackberries, Bluetooth-Geräte und externe Festplatten. Der Gerätemanager kann den Anschluss nicht autorisierter Geräte an die Anschlüsse Ihres Computers auch generell unterbinden.

Program Security Guard

Program Security Guard kann abhängig von der Konfiguration, die Ihr SystemAdministrator gewählt hat, verhindern, dass Sie bestimmte Dateitypen auf Ihrem Computer oder auf Netzwerkgeräten erstellen können. Program Security Guard kann auch verhindern, dass Sie bestimmte Dateien verändern oder löschen.

Die geschützten Dateitypen werden nach Erweiterung angegeben und sind ein Mittel, um das Ändern nicht lizenzierter oder nicht autorisierter Software (.exe, .com, .dll usw.), potenziell gefährlicher Dateitypen (.vbs, .scr usw.) oder einfach nicht erwünschter Dateitypen (.mpg, .mp3, .mov, .avi usw.) zu verhindern. Dieser Schutz gilt für alle externen Quellen, darunter E-Mail-Anhänge und Internet-Downloads.

Zwischengespeicherte Kennwörter

Wenn Ihr Computer mit dem Unternehmensnetzwerk verbunden ist, können Sie normalerweise automatisch auf Daten zugreifen, die auf Wechselmedien gespeichert sind, ohne ein Kennwort eingeben zu müssen. Wenn Sie versuchen, auf diese Daten zuzugreifen, wenn Sie nicht mit dem Unternehmensnetzwerk verbunden sind oder auf einem Computer arbeiten, auf dem Media Encryption nicht installiert ist, werden Sie möglicherweise zur Eingabe eines Kennworts aufgefordert.

Wenn Ihr SystemAdministrator die Funktion zum Zwischenspeichern von Kennwörtern aktiviert hat, bietet Media Encryption die Möglichkeit, das Kennwort bei der ersten Eingabe zu speichern. Wenn Sie das nächste Mal auf das Gerät zugreifen, können Sie das gespeicherte Kennwort verwenden, ohne es erneut eingeben zu müssen.

Wenn Sie einen verschlüsselten Datenträger in Ihren Computer einlegen oder ein verschlüsseltes Gerät anschließen, wird das Dialogfeld **Zugriffssteuerung** geöffnet.

So speichern Sie ein Kennwort:

Wählen Sie die Optionen **Kennwort eingeben** und **Kennwort zwischenspeichern**, und geben Sie ein Kennwort ein, dass der KennwortRichtlinie Ihres Unternehmens entspricht. Klicken Sie anschließend auf **OK**.

So verwenden Sie ein bereits gespeichertes Kennwort:

Wählen Sie die Option **Zwischengespeichertes Kennwort verwenden**, und klicken Sie auf **OK**. Es wird in Klammern der Text 'Uneingeschränkter Zugriff' oder 'Lesezugriff' angezeigt, nachdem Sie auf **Zwischengespeichertes Kennwort verwenden** geklickt haben. Diese Informationen geben an, ob Sie mit dem gespeicherten Kennwort uneingeschränkten Zugriff oder nur Lesezugriff auf das verschlüsselte Medium haben.

So ändern Sie ein bereits gespeichertes Kennwort:

Wählen Sie **Kennwort eingeben** und **Kennwort zwischenspeichern**, und geben Sie das alte Kennwort ein. Klicken Sie anschließend auf **OK**. Es wird ein neues Dialogfeld angezeigt, das Sie zum Festlegen eines neuen Kennworts auffordert.

Grau hinterlegte Optionen

Einige Optionen im Kennwort-Dialogfeld sind möglicherweise aus folgenden Gründen grau hinterlegt:

Grau hinterlegt:	Grund:
'Zwischengespeichertes Kennwort verwenden' und 'Kennwort zwischenspeichern'	Die Funktion zum Zwischenspeichern von Kennwörtern wurde von Ihrem SystemAdministrator nicht aktiviert, oder

	Sie greifen zum ersten Mal auf das Medium zu, und es wurde zuvor kein Kennwort festgelegt.
'Zwischengespeichertes Kennwort verwenden'	Es befindet sich kein zwischengespeichertes Kennwort im Zwischenspeicher. Das Kennwort wurde möglicherweise nicht gespeichert oder das Kennwort wurde geändert. Bei einer Kennwortänderung wurde das alte Kennwort aus dem Zwischenspeicher gelöscht, und das neue Kennwort wurde noch nicht gespeichert.
'Kennwort zwischenspeichern'	Sie müssen Ihr Kennwort ändern. Das Kontrollkästchen Kennwort zwischenspeichern ist grau hinterlegt, weil das alte Kennwort nicht gespeichert werden muss.

Verwenden des EPM Clients

In diesem Abschnitt wird beschrieben, wie Sie wechselbare Speichermedien verschlüsseln, entschlüsseln und verwalten.

Media Encryption schützt wechselbare Speichermedien durch Verschlüsseln des gesamten Speicherbereichs oder eines Teils des Speichers auf dem Medium und anschließendes Ablegen von Informationen in diesem verschlüsselten Bereich. Die Verschlüsselung und Verwaltung von Wechselmedien erfolgt mit dem EPM Client (Encryption Policy Manager).

Um mit dem EPM Client zu arbeiten, klicken Sie auf der Media Encryption-Seite im Bereich für den EPM Client auf **Öffnen**.

Das Fenster für den EPM Client wird geöffnet. Die verbundenen Wechselmediengeräte werden links im Bildschirm aufgeführt.

Verschlüsseln von Medien

Die Richtlinie in Ihrem Unternehmen kann so konfiguriert werden, dass nur der Zugriff auf verschlüsselte Medien zulässig ist. In diesem Fall wird ein Verschlüsselungsprozess gestartet, sobald Sie ein unverschlüsseltes Medium in Ihren mit Media Encryption geschützten Computer einlegen. Sie können einen Verschlüsselungsprozess auch manuell starten.

In beiden Fällen führt ein Assistent Sie durch den Verschlüsselungsprozess. Bei diesem Prozess wird ein verschlüsselter Speicherbereich auf dem Gerät erstellt. Dieser Schritt wird als Import bezeichnet.

Sie können die Größe des zu verschlüsselnden Bereichs auf dem Gerät als Prozentwert festlegen. Wenn Sie beispielsweise den Wert 50 % wählen, erstellt Media Encryption einen verschlüsselten Container, dessen Größe der Hälfte des gesamten Speicherbereichs entspricht. Wenn Sie Dateien importieren und verschlüsseln, werden die Dateien immer in diesem Container abgelegt.



Hinweis – Wenn Sie einen Bereich definieren, der für die hier zu speichernden Daten nicht ausreicht, schlägt die Verschlüsselung fehl.

So verschlüsseln Sie Medien:

1. Starten Sie den Assistenten, indem Sie ein Wechselmedium oder eine CD/DVD in Ihren Computer einlegen, oder klicken Sie im Fenster **EPM Client** auf **Import**, wenn der Assistent nicht automatisch startet. Klicken Sie auf **Weiter**.



Wichtig – Es ist nicht ratsam, Wechselmedien zu verschlüsseln, die in externen, nicht computerbasierten Geräten verwendet werden, zum Beispiel Digitalkameras, iPods, MP3-Player usw. In solchen Fällen wird eine Meldung angezeigt, und das Medium erhält nur Lesezugriff. Wenn die Verschlüsselung gestartet wurde, warten Sie bis zum Abschluss des Vorgangs. Entschlüsseln Sie das Medium anschließend, indem Sie auf **Export** klicken.

2. Geben Sie im Fenster **Medieneigenschaften** den zu verschlüsselnden Prozentsatz des Mediums ein. Klicken Sie auf **Weiter**.



Hinweis – Bei CDs oder DVDs ist es nicht möglich, nur einen Teil der Disk zu verschlüsseln. Daher ist diese Einstellungen grau hinterlegt.

3. Definieren Sie im Fenster **Informationen zum Medieneigentümer** den Eigentümer des Mediengeräts, indem Sie eine der folgenden Optionen auswählen:

- **Medieneigentümer wird bei erster Verwendung zugewiesen:** Der erste Benutzer, der das Medium in einen Endpunkt-Computer einlegt, wird automatisch zum Eigentümer.
- **Medium einem Benutzer zuweisen:** Weisen Sie die Eigentümerschaft dem Benutzer (also sich selbst) zu, der die Verschlüsselung ausführt, oder klicken Sie auf **Durchsuchen**, um einen Benutzer aus der aktiven Domäne auszuwählen.



Hinweis – Wenn Sie CDs/DVDs verschlüsseln, ist nur die Option **Medium einem Benutzer zuweisen** verfügbar.

4. Klicken Sie auf **Weiter**.

5. Geben Sie im Fenster für den Kennwortschutz ein Kennwort für den Zugriff ein, und bestätigen Sie es. Kennwörter müssen den Regeln entsprechen, die von Ihrem SystemAdministrator eingerichtet wurden. Klicken Sie auf **Weiter**.

Das Kennwort bietet Benutzern, bei denen Media Encryption nicht installiert ist, die Möglichkeit, auf die Informationen auf dem Gerät oder dem Datenträger zuzugreifen. Wenn Sie sich an dieser Stelle gegen das Einrichten eines Kennworts entscheiden, können Sie nur auf den Datenträger zugreifen, wenn Sie im aktuellen Netzwerk (oder in einem anderen von Ihrem SystemAdministrator festgelegten Netzwerk) angemeldet sind und Ihr SystemAdministrator den automatischen Zugriff auf Medien aktiviert hat.

6. Wenn Sie eine CD/DVD verschlüsseln, können Sie in einem Fenster die Dateien auswählen, die in den verschlüsselten Bereich auf der Disk importiert oder aus diesem entfernt werden sollen.
 - a. Wechseln Sie in der Ordnerstruktur auf die nächsthöhere Ebene.
 - b. Wählen Sie Dateien oder einen ganzen Ordner für das Brennen auf die Disk aus.
 - c. Markieren und löschen Sie Dateien oder Ordner, die nicht auf der Disk enthalten sein sollen. Klicken Sie auf **Weiter**. Die Dateien werden importiert und die Disk gebrannt.
 - d. Es wird eine Meldung angezeigt, sobald der Brennvorgang abgeschlossen ist.
7. Im Fortschrittsfenster können Sie den Verschlüsselungsvorgang verfolgen. Je nach Art des Mediums und Menge der Daten kann dieser Vorgang viel Zeit in Anspruch nehmen.



Wichtig – Entfernen Sie das Speichergerät unter **KEINEN** Umständen während des Verschlüsselungsvorgangs. Sie zerstören damit Ihre Daten und beschädigen unter Umständen das Medium.

8. Wenn das Fenster **Fertig** geöffnet wird, klicken Sie auf **Fertig stellen**, um den Vorgang abzuschließen. Das Fenster **EPM Client** wird wieder angezeigt.

Beachten Sie, dass als Status für das verschlüsselte Medium nun **Verschlüsselt** angezeigt wird und dass die Schaltfläche **Importieren** nicht mehr verfügbar ist.

Folgende Informationen werden für das ausgewählte Gerät angezeigt:

- **EPM-Status:** Der aktuelle Status des ausgewählten verschlüsselten Geräts.
- **Mediengröße:** Die Größe des ausgewählten Geräts.

- **Erstellungsdatum:** Das Datum, an dem das ausgewählte verschlüsselte Laufwerk erstellt wurde.
- **Zugriffsdatum:** Das Datum des letzten Zugriffs auf das ausgewählte verschlüsselte Laufwerk.
- **Eigentümer:** Die Benutzer-ID des Benutzers, der das verschlüsselte Gerät erstellt hat.



Hinweis – Es wird empfohlen, zum Trennen verschlüsselter Medien von Ihrem Computer immer die Funktion **Hardware sicher entfernen** zu verwenden, um eine Beschädigung der Medien zu vermeiden. Klicken Sie im Infobereich der Taskleiste auf das Symbol zum sicheren Entfernen von Hardware, und wählen Sie das zu trennende Medium aus.

Verschlüsseln von CDs und DVDs

Wenn Ihre Richtlinie es zulässt, kann Media Encryption CDs und DVDs mit folgenden Voraussetzungen bzw. Einschränkungen verschlüsseln:

- CDs können unter Windows XP und Windows Vista verschlüsselt werden.
- DVDs können unter Windows Vista verschlüsselt werden.
- Die Verschlüsselung kann nur mit RW- und unbeschriebenen R/RW-Disks ausgeführt werden.
- Einmal gebrannten CDs/DVDs können keine Daten hinzugefügt bzw. von diesen entfernt werden. Sie können solche Disks nur vollständig löschen.

Das Importieren und Exportieren von Dateien auf bzw. von CDs/DVDs erfolgt ähnlich wie bei anderen im Abschnitt **Verschlüsseln von Medien** auf Seite 139 beschriebenen Wechselmedien. Zwischen CDs/DVDs und anderen Wechselmedien bestehen zwei Unterschiede: Sie können bei CDs/DVDs keinen separaten Bereich verschlüsseln, und Sie können nach dem Brennen der Disk keine Dateien hinzufügen oder löschen. Wenn Sie Daten von einem wiederbeschreibbaren Datenträger entfernen möchten, müssen Sie ihn mit der Funktion **Löschen** vollständig löschen.

Zugreifen auf verschlüsselte Medien

Zum Schutz von Informationen erstellt Media Encryption auf Ihrem Wechseldatenträger einen verschlüsselten Bereich, in dem alle Daten abgelegt

werden. Um auf die Daten in diesem geschützten Bereich zuzugreifen, können Sie diese entschlüsseln oder exportieren. Normalerweise erlaubt Ihre Media Encryption-Richtlinie nur dem Besitzer oder einem autorisierten Benutzer, die Entschlüsselung durchzuführen.

Entschlüsseln:

Der Media Encryption Client liest die auf dem Medium gespeicherten Informationen, diese verbleiben jedoch im geschützten Bereich. Dies geschieht normalerweise, wenn Sie von Ihrem Computer auf das Medium zugreifen, wenn dieses mit dem Unternehmensnetzwerk verbunden ist. Wenn Sie nicht mit dem Netzwerk verbunden sind oder versuchen, von einem Computer ohne Media Encryption auf das Medium zuzugreifen, müssen Sie möglicherweise ein Kennwort eingeben.

Exportieren:

Exportieren bedeutet, dass Media Encryption die Daten aus dem verschlüsselten Bereich extrahiert und den verschlüsselten Bereich entfernt. Das Medium ist dann nicht mehr verschlüsselt.

So entschlüsseln Sie Wechselmedien:

1. Legen Sie Ihr verschlüsseltes Medium in Ihren Computer ein.
2. Wenn Sie nicht automatisch auf das Medium zugreifen können, müssen Sie gegebenenfalls ein Kennwort eingeben. Geben Sie im Fenster **Kennwort** das entsprechende Kennwort ein, oder verwenden Sie ein gespeichertes Kennwort. Klicken Sie auf **OK**.
3. Sie können jetzt auf die Dateien zugreifen. Da sie nicht verschlüsselt sind, können Sie die Dateien vom Medium auf Ihre Festplatte kopieren.

So exportieren Sie Informationen von einem Wechselmedium:

1. Legen Sie Ihr verschlüsseltes Medium in Ihren Computer ein.
2. Öffnen Sie den **EPM Client**, und klicken sie auf **Exportieren**. Der Assistent für den EPM-Medienexport wird geöffnet.
3. Wenn Sie nicht automatisch auf das Medium zugreifen können, müssen Sie gegebenenfalls ein Kennwort eingeben. Geben Sie im Fenster **Kennwort** das entsprechende Kennwort ein, oder verwenden Sie ein gespeichertes Kennwort. Klicken Sie auf **OK**.
4. Klicken Sie auf **Fertig stellen**, um den Vorgang zu beenden. Die **Entschlüsselung** kann abhängig von der Größe und dem Typ des Geräts einige Zeit in Anspruch nehmen. Nach Abschluss der Entschlüsselung ist der verschlüsselte Bereich

entschlüsselt und wird entfernt. Die Daten auf dem Medium sind jetzt entschlüsselt und nicht mehr geschützt.



Wichtig – Entfernen Sie das Speichermedium unter **KEINEN** Umständen während des Verschlüsselungsvorgangs. Sie zerstören damit Ihre Daten und beschädigen unter Umständen das Medium.

Zugreifen auf verschlüsselte Medien von Computern ohne Media Encryption

Wenn Ihr Profil den Zugriff auf verschlüsselte Informationen von Computern ohne Media Encryption gestattet, wird während der Verschlüsselung automatisch eine unlock.exe Datei in das Stammverzeichnis des Wechselmediums kopiert.



Hinweis – Sie müssen bei der Verschlüsselung ein Kennwort festlegen, um von Computern ohne Media Encryption auf die Informationen zugreifen zu können.

So entschlüsseln Sie Wechselmedien offline:

1. Legen Sie das verschlüsselte Medium in einen Computer ein, auf dem Media Encryption nicht ausgeführt wird. Es werden folgende Dateien angezeigt: dvrem.epm, autorun.exe und unlock.exe.

Dvrem.epm ist der verschlüsselte Speicher, autorun.exe führt die Datei zum Aufheben der Sperre aus, und unlock.exe entschlüsselt den verschlüsselten Speicher.
2. Um auf verschlüsselte Daten auf dem Gerät zuzugreifen, doppelklicken Sie auf die Datei unlock.exe (auf den meisten Systemen wird sie automatisch ausgeführt). Geben Sie das Kennwort ein.
3. Der Encryption Richtlinie Manager Explorer wird geöffnet und zeigt den Inhalt des verschlüsselten Geräts an.
4. Für den Zugriff auf die Daten auf dem verschlüsselten Gerät stehen zwei Methoden zur Verfügung: Extrahieren der Dateien auf die lokale Festplatte oder in einen sicheren Bereich auf dem Gerät selbst. Eine Beschreibung dieser beiden Methoden finden Sie im Folgenden.

Wenn Sie ein Kennwort für uneingeschränkten Zugriff verwenden, können Sie jetzt per Drag-and-Drop oder durch Kopieren Dateien von dem verschlüsselten Gerät bewegen. Wenn Sie ein Kennwort für Lesezugriff verwenden, können Sie die Informationen auf dem Gerät nur lesen, jedoch keine Dateien von diesem Gerät bewegen oder kopieren.

Extrahieren von Dateien auf die lokale Festplatte

Sie können Dateien und Ordner aus dem verschlüsselten Bereich extrahieren und diese auf einer lokalen Festplatte oder Netzwerklaufwerk speichern.

So extrahieren Sie Dateien auf Ihre Festplatte oder ein Netzwerklaufwerk:

1. Wählen Sie die Dateien oder Ordner aus, die Sie entschlüsseln und auf einer lokalen Festplatte speichern möchten. Verwenden Sie hierzu **STRG** und die **Umschalttaste**, und klicken Sie im mit der rechten Maustaste geöffneten Kontextmenü auf **Extrahieren**.
2. Wählen Sie den Speicherort für die Dateien aus.
Die Dateien werden jetzt entschlüsselt und als reiner Text an dem gewählten Speicherort abgelegt.
3. Wenn Sie den EPM Explorer schließen, werden Sie gefragt, ob alle extrahierten Dateien sicher gelöscht werden sollen. Wenn Sie auf **Ja** klicken, werden alle neu extrahierten Dateien sicher gelöscht, sodass keine Spuren der sensiblen Informationen verbleiben.

Extrahieren von Dateien in einen sicheren temporären Speicherort

So extrahieren Sie Dateien in einen sicheren temporären Speicherort:

- Doppelklicken Sie im Laufwerks-Explorer auf die Datei.
Der EPM Explorer entschlüsselt die Datei in einen temporären Speicherort und öffnet sie automatisch mit der verbundenen Anwendung.

So zeigen Sie eine Datei im sicheren Modus an:

- Doppelklicken Sie auf die erforderliche Datei.
Wenn Sie Änderungen an der verschlüsselten Datei vornehmen, werden Sie gefragt, ob Sie die verschlüsselte Datei auf dem Gerät aktualisieren möchten. Klicken Sie auf **Ja**, wenn Sie die Datei speichern möchten.

Löschen von CDs oder DVDs

Wenn eine verschlüsselte CD oder DVD gebrannt wurde, gibt es keine Möglichkeit, einzelne Dateien auf diesen Datenträgern zu löschen. Die einzige Möglichkeit besteht darin, alle auf der Disk gespeicherten Informationen zu entfernen.

Um eine Disk zu löschen, klicken Sie im EPM auf Löschen.

Ändern des Kennworts für das verschlüsselte Gerät

So ändern Sie das Zugriffskennwort für Wechselmedien für ein verschlüsseltes Gerät:

1. Wählen Sie das jeweilige Gerät auf der linken Seite des Fensters EPM Client aus.
2. Klicken Sie auf Festlegen. Das Fenster Kennwort wird geöffnet.
3. Geben Sie das alte Kennwort ein, und klicken Sie auf OK.

Wenn Sie ein Kennwort für den uneingeschränkten Zugriff eingegeben haben, können Sie sowohl Kennwörter für uneingeschränkten Zugriff als auch Kennwörter für Lesezugriff ändern. Wenn Sie ein Kennwort für Lesezugriff eingeben, können Sie nur Kennwörter für Lesezugriff ändern.



Hinweis – Kennwörter für uneingeschränkten Zugriff und Kennwörter für Lesezugriff dürfen nicht identisch sein.

4. Geben Sie das neue Kennwort ein, und bestätigen Sie es.



Hinweis – Das Kennwort muss den vom Administrator definierten Kriterien entsprechen, auf die Sie zugreifen, indem Sie auf Richtlinienhinweis klicken.

5. Klicken Sie auf OK.

Verwenden des Managers für Wechselmedien

Sie können den Zugriff auf Wechselmedien und Geräte wie Disketten, externe Laufwerke (FAT-formatiert), PDAs, Flash-Speicher, Digitalkameras usw. steuern.

Wenn der Manager für Wechselmedien aktiviert ist, müssen alle Wechselmedien (außer CDs und DVDs) autorisiert sein, bevor Sie auf diese zugreifen können.

Autorisieren von Wechselmedien

Wenn Sie Wechselmedien autorisieren dürfen, wird eine Warnung angezeigt:

So autorisieren Sie das Wechselmediengerät in diesem Fenster:

1. Klicken Sie auf **Autorisieren**.

Der Assistent für den Medienimport wird geöffnet und führt Sie durch die Schritte der Autorisierung.

2. Klicken Sie auf **Ignorieren**, um das Fenster mit dieser Warnung zu schließen. Der Zugriff auf das Wechselmedium ist dann nicht möglich.

Wenn Sie die Berechtigung besitzen, können Sie Wechselmedien auch autorisieren, indem Sie im Bereich des Managers für Wechselmedien von Media Encryption die Option **Scan** wählen. Der Assistent für den Medienimport wird geöffnet.

So autorisieren Sie Wechselmedien mit dem Assistenten für den Medienimport:

1. Klicken Sie im Begrüßungsbildschirm auf **Weiter**, um fortzufahren.

Im Fenster für die Virens Scanner sind entweder alle entdeckten Virens Scanner auf Ihrem Computer ausgewählt, oder Sie können Virens Scanner selbst auswählen. Die Virens Scanner stellen sicher, dass das Wechselmedium virenfrei ist und nur die autorisierten Dateitypen enthält.

2. Wenn die Richtlinie das Auswählen von Virens Scannern erlaubt, wählen Sie die Scanner aus, die Sie ausführen möchten.

Wenn die Richtlinie das Überspringen des Scanvorgangs erlaubt, d. h. Autorisieren von Wechselmedien ohne vorheriges Scannen, können Sie die Option **Scan überspringen** wählen. Dies ist allerdings nicht empfehlenswert.

3. Klicken Sie auf **Weiter**.

Wenn ein Virens Scan durchgeführt wurde, wird ein Fenster mit der Meldung angezeigt, ob das Wechselmedium den Scan bestanden hat. Ist der Scan fehlgeschlagen, wird der Zugriff auf das Wechselmedium gesperrt.

4. Wenn das Fenster **Fertig** angezeigt wird, klicken Sie auf **Fertig stellen**.

Verwenden des Gerätemanagers

Der Media Encryption-Gerätemanager steuert den Zugriff auf Geräte, die mit den verschiedenen Anschlüssen Ihres Computers verbunden sind. Die Media Encryption-Richtlinie gibt an, welchen Geräten Zugriff gewährt wird und welche Art von Zugriff zulässig ist (Lesezugriff, Lese-/Schreibzugriff, Zugriff mit Ausführungsrecht).

Die Benutzeroptionen des Gerätemanagers befinden sich im Bereich **Gerätemanager** der Seite Media Encryption.

Um die Richtlinienregeln für verschiedene Geräte anzuzeigen, klicken Sie auf **Anzeigen**.

Wenn die Regeln des Gerätemanagers den Zugriff auf ein Gerät oder einen Port sperren, wird eine Warnung angezeigt.

Verwenden von Program Security Guard

Program Security Guard kann verhindern, dass Sie bestimmte Dateitypen auf Ihrem Computer oder auf einem Netzwerklaufwerk ändern. Weitere Informationen zu Program Security Guard finden Sie im Abschnitt zu Program Security Guard.

Wenn Program Security Guard den Zugriff auf eine Datei sperrt, wird eine Meldung angezeigt.

Bereich "Wartung"

Im Bereich **Wartung** der Seite Media Encryption können Sie die Media Encryption-Richtlinie manuell aktualisieren und die Verbindungsfähigkeit mit dem Media Encryption-Server testen.

Um die Media Encryption-Richtlinie zu aktualisieren, klicken Sie auf **Aktualisieren**.

Zum Testen der Netzwerkverbindung mit dem Media Encryption-Server klicken Sie auf **Testen**. Diese Funktion ist nützlich, wenn Sie Probleme mit der Verbindung zwischen Client und Server diagnostizieren möchten.

WebCheck

WebCheck bietet umfassenden Schutz gegen zahlreiche Bedrohungen, denen Ihr Computer und Ihr Unternehmensnetzwerk im Internet ausgesetzt sind.

Wenn Ihr Administrator Ihre Endpoint Security-Richtlinie für die Verwendung von WebCheck konfiguriert hat, steht diese Funktion in Ihrem Endpoint Security Client zur Verfügung.

Inhalt dieses Abschnitts

[Grundlegendes zu WebCheck](#)

149

[Warnungen vor verdächtigen Sites](#)

151

Grundlegendes zu WebCheck

WebCheck erweitert Endpoint Security Antivirus um eine zusätzliche Ebene zum Schutz gegen Web-basierte Bedrohungen und bietet die Firewall zum Schutz vor PC-basierten Bedrohungen.

Schutz durch WebCheck

Ihr Administrator bestimmt, welche WebCheck-Einstellungen zum Schutz Ihres Computers vor Web-basierten Bedrohungen erforderlich sind. In der folgenden Liste sind die Funktionen von WebCheck erläutert.

- **Unternehmensmodus:** Ihr Browser wird automatisch im Unternehmensmodus geöffnet, wenn Sie die Website Ihres Unternehmens oder Internet-Websites besuchen, die Ihr Administrator als vertrauenswürdig erachtet. Die WebCheck-Funktionen sind nicht aktiv, weil von diesen Websites nicht dieselben Gefahren ausgehen wie vom Internet insgesamt. Ihr Administrator konfiguriert, welche Sites im Unternehmensmodus sicher geöffnet werden können.

- **Virtualisierung:** WebCheck fängt Malware und andere unerwünschte Programme ab, die ohne Ihre Erlaubnis oder Kenntnis auf Ihren Computer heruntergeladen werden, und sperrt diese in einem virtuellen Dateisystem ein, sodass diese Ihre realen Computer-Festplatten nicht erreichen.
- **Anti-Datenlogger:** WebCheck verschlüsselt Ihre Tastatureingaben, sodass von einem Datenlogger abgefangene Informationen nicht lesbar sind. Des Weiteren sperrt WebCheck auch Systeminformationen, die Screen Grabbing-Programme nutzen.
- **Anti-Phishing (Signatur):** WebCheck verfolgt aktuell erkannte Phishing- und Spionage-Sites. Wenn Sie eine solche Site aufrufen, unterbricht WebCheck den Seitenaufruf mit einer Warnmeldung, sodass Sie die Site sofort verlassen können.
- **Anti-Phishing (Heuristik):** WebCheck verwendet außerdem heuristische Regeln, die nach bestimmten Merkmalen betrügerischer Seiten suchen, um Phishing-Sites zu erkennen, die erst Sekunden zuvor erstellt wurden.
- **Sperren von Spyware-Websites:** WebCheck sperrt Websites, die in seiner Datenbank bekannter Sites für die Spyware-Verbreitung enthalten sind.

Internet-Modus und Unternehmensmodus

WebCheck wird in zwei Modi ausgeführt: **Internet-Modus** und **Unternehmensmodus**. WebCheck erkennt, wenn Sie von einer internen Website zu einer externen Site im Internet (und umgekehrt) wechseln und öffnet einen neuen Browser im entsprechenden Modus.

Internet-Modus

Ihr Browser wird automatisch im Internet-Modus geöffnet, wenn Sie Websites außerhalb Ihres Unternehmensnetzwerkes besuchen. Alle auf Ihrem Computer konfigurierten WebCheck-Schutzfunktionen sind aktiv.

Wenn Sie im Internet-Modus surfen, erstellt WebCheck einen temporären, isolierten Bereich, in dem Malware gefangen und gelöscht wird, bevor sie Ihr reales Computersystem erreicht.

Wenn Sie Inhalte herunterladen möchten, lässt der Virtualisierungsschild Ihre Datei durch, die dann auf Ihrem Computer gespeichert werden kann. Aus diesem Grund bietet Endpoint Security weitere Funktionen, um betrügerische Sites zu erkennen.

Unternehmensmodus

Ihr Browser wird automatisch im Unternehmensmodus geöffnet, wenn Sie die Website Ihres Unternehmens aufrufen. Die meisten WebCheck-Funktionen sind nicht aktiv, weil von der Website Ihres Unternehmens nicht dieselbe Gefahr ausgeht wie von externen Internet-Websites.

Wechseln zwischen den Modi

Der aktuelle Modus wird immer in der Titelleiste Ihres Browsers angezeigt.

Wenn Sie von einer internen Website (Unternehmensmodus) auf eine externe Website (Internet-Modus) oder umgekehrt wechseln, weist eine Meldung Sie auf den Moduswechsel hin. Klicken Sie auf OK, um das Meldungsfeld zu schließen.

Wenn WebCheck den Moduswechsel ohne Benachrichtigung ausführen soll, wählen Sie **In Zukunft keine Benachrichtigung anzeigen**. Sites automatisch im entsprechenden Modus öffnen., wenn die Benachrichtigung angezeigt wird.

Warnungen vor verdächtigen Sites

Wenn WebCheck bei einer von Ihnen besuchten Website ein Sicherheitsproblem feststellt, werden Sie sofort vor der bestehenden Gefahr gewarnt, sodass Sie die Site gefahrlos verlassen können.

Wenn eine Site beispielsweise als Phishing-Site oder Spyware-Verteiler bekannt ist, wird die WebCheck-Symbolleiste rot dargestellt und der Seitenaufruf mit einer Warnung unterbrochen. Bei Sites, die fragwürdig erscheinen, jedoch erwiesenermaßen nicht gefährlich sind, wird unter der Symbolleiste eine Meldeleiste angezeigt.

Klicken Sie im Warnungsdialogfeld auf den Link **Weitere Informationen**, um sicherheitsrelevante Informationen zu der Site zu erhalten, beispielsweise ob es sich um eine bekannte Phishing-Site oder einen Spyware-Verteiler handelt, das Erstellungsdatum der Site und den Hosting-Ort der Site.

Gelber Meldebanner

Wenn Sie eine Webseite besuchen, die keine ausreichenden Sicherheitszertifikate besitzt, erscheint eine gelbe Meldeleiste unter der Symbolleiste.

Diese Site ist möglicherweise nicht gefährlich. Möglicherweise ist sie neu oder hat nur ein beschränktes Budget und kann daher keine ausreichende Sicherheitszertifizierung (SSL-Zertifikat) erwerben. Trotzdem bedeutet das Fehlen

von Sicherheitseinrichtungen auf der Site, dass Daten abgefangen werden können. Sie sollten daher auf die Eingabe sensibler Daten verzichten.

Risikostufe von Websites	MEDIUM für Eingabe von Daten oder Herunterladen von Dateien von dieser Site.
Empfehlung	Bei aktivem WebCheck sollte eine Anzeige der Site sicher sein. Geben Sie jedoch keine sensiblen Daten ein, und laden Sie keine Dateien von dieser Site herunter.
Warum ist die Site fragwürdig?	Klicken Sie im Warnungsdialogfeld auf den Link Weitere Informationen , um sicherheitsrelevante Informationen zu der Site zu erhalten.

Rote Warnung "Könnte Phishing sein"

Wenn Sie eine Webseite besuchen, auf der die heuristischen Erkennungsfunktionen von WebCheck Merkmale von Phishing entdecken, wird das Surfen durch eine rote Warnung **Könnte eine Phishing-Site sein** unterbrochen.

Obwohl die Site Merkmale von Phishing aufweist, wurde sie noch nicht offiziell als solche Site gemeldet. Es könnte sich um eine neue, noch nicht entdeckte Phishing-Site handeln. Die Site könnte jedoch auch sicher sein.

Folgende Empfehlungen sollen Ihnen bei der Entscheidung helfen, ob diese Site vertrauenswürdig ist.

Table 0-25 Rote Warnung "Könnte Phishing sein"

Risikostufe von Websites	MEDIUM bis HOCH für Eingabe von Daten oder Herunterladen von Dateien von dieser Seite.
Empfehlungen	Diese Seite ist möglicherweise keine Phishing-Site, wir empfehlen Ihnen jedoch auf Zurück zu klicken, wenn Folgendes zutrifft: Sind Sie durch Klicken auf einen Link in einer E-Mail auf diese Seite gelangt? Beginnt die Adresse statt mit https mit http? Sites, die nach persönlichen Daten fragen, sollten durch zusätzliche Verschlüsselung und Authentifizierung (angezeigt durch https) gesichert sein. Gibt es einen Fehler in der Seitenadresse, z. B. "yahooo" statt "yahoo"? Klicken Sie im Warnungsdialogfeld auf den Link Weitere Informationen, um sicherheitsrelevante Informationen zu der Site zu erhalten. Ist im Info-Dialogfeld der Website ein Erstellungsdatum für die Site angegeben, das noch nicht lange zurückliegt, oder erfolgt das Hosting der Site in einem unerwarteten Land?
Warum ist die Site fragwürdig?	Die heuristische Prüfung hat einige Merkmale gefunden hat, die für Phishing üblich sind, die Seite wurde jedoch nicht offiziell als Phishing-Site gemeldet.

Rote Warnmeldungen

Wenn Sie eine Site aufrufen, die bekanntermaßen gefährlich ist, unterbricht WebCheck den Seitenaufruf mit einer Warnung, und die WebCheck-Symbolleiste wird rot dargestellt.

Table 0-26 Rote Warnung

Risikostufe von Websites	SEHR HOCH
Empfehlung	Wenn dies eine Phishing-Site ist, verlassen Sie diese sofort, um Ihren Computer und Ihr Netzwerk zu schützen. Wenn es sich um eine Spyware-Verteilerseite handelt, schützt Sie WebCheck, solange Sie keine Daten eingeben oder Daten herunterladen. Klicken Sie auf die Schaltfläche Zurück, um die Seite sicher zu verlassen.
Weitere Informationen	Klicken Sie im Warnungsdialogfeld auf den Link Weitere Informationen , um sicherheitsrelevante Informationen zu der Site zu erhalten.

E-Mail-Schutz

Würmer, Viren und andere Bedrohungen infizieren Computer oft über E-Mails. MailSafe schützt Ihre Kontakte, indem es verhindert, dass Malware über Ihre E-Mails verbreitet wird.

MailSafe schützt nur Nachrichten des SMTP-Protokolls.

Inhalt dieses Abschnitts

Schutz für ausgehenden MailSafeverkehr	155
Schutz für ausgehenden MailSafeverkehr	156
Anpassen des MailSafe-Schutzes für ausgehenden Datenverkehr	156

Schutz für ausgehenden MailSafeverkehr

Der MailSafe-Schutz für ausgehenden MailSafeverkehr warnt Sie, wenn Ihr E-Mail-Programm versucht, eine ungewöhnlich große Anzahl an Nachrichten zu versenden (über fünf E-Mail-Nachrichten innerhalb von zwei Sekunden), oder den Versuch unternimmt, eine E-Mail-Nachricht an eine ungewöhnlich große Anzahl von Empfängern zu senden (über fünfzig Empfänger). Dadurch kann Ihr Computer nicht ohne Ihr Wissen zum Versenden von infizierten Anhängen verwendet werden. Zudem wird mit dem MailSafe-Schutz für ausgehenden MailSafeverkehr sicher gestellt, dass das Programm, das versucht, die E-Mail-Nachrichten zu versenden, auch über die notwendigen Rechte zum Versenden von E-Mails verfügt.

Der MailSafe-Schutz für ausgehenden MailSafeverkehr funktioniert mit den folgenden E-Mail-Anwendungen:

- Eudora
- Outlook
- Outlook Express

- Netscape Mail
- Pegasus Mail
- Juno

Schutz für ausgehenden MailSafeverkehr

Der E-Mail-Schutz für ausgehenden Datenverkehr ist zu Ihrer Sicherheit standardmäßig aktiviert. Wenn der Schutz für ausgehenden Datenverkehr aktiviert ist, werden die MailSafe-Einstellungen für ausgehenden MailSafeverkehr für alle Programme mit Berechtigungen zum Senden von E-Mails aktiviert.

So aktivieren Sie den E-Mail-Schutz für ausgehenden Datenverkehr:

1. Öffnen Sie E-Mail-Schutz|Grundeinstellungen.
2. Wählen Sie im Bereich Schutz für ausgehende E-Mails die Option Ein.

Anpassen des MailSafe-Schutzes für ausgehenden Datenverkehr

Sie können selbst festlegen, wann MailSafe aktiviert wird. Sie können das Zeitintervall erweitern, die Anzahl der zulässigen Nachrichten und Empfänger erhöhen oder die E-Mail-Adressen angeben, die von Ihrem Computer aus E-Mail-Nachrichten senden dürfen.

MailSafe nach Programm aktivieren

Wenn der E-Mail-Schutz für ausgehenden MailSafeverkehr aktiviert ist, gilt dieser Schutz für alle Programme, die berechtigt sind, E-Mail-Nachrichten zu senden.

Sie können den MailSafe-Schutz für ausgehenden Datenverkehr anpassen, indem Sie ihn für bestimmte Programme aktivieren oder deaktivieren.

Weitere Informationen zum Einstellen der Berechtigungen für ein Programm finden Sie unter **Einstellen spezifischer Berechtigungen** auf Seite [103](#).

So aktivieren Sie den MailSafe-Schutz für ausgehende E-Mails für ein Programm:

1. Öffnen Sie Program ControllProgramme.
2. Klicken Sie in der Spalte Programme mit der rechten Maustaste auf einen Programmnamen, und wählen Sie dann Optionen aus.

3. Öffnen Sie die Registerkarte Sicherheit.
4. Aktivieren Sie im Bereich Schutz für ausgehende E-Mails das Kontrollkästchen Schutz für ausgehende E-Mail für dieses Programm aktivieren.
5. Klicken Sie auf OK.

Schutz für ausgehenden MailSafeverkehr

Damit ungefährliche E-Mail-Nachrichten, die normalerweise MailSafe auf Grund von zu vielen Empfängern oder Übermittlungen aktivieren würden, gesendet werden können, lassen sich die MailSafe-Schutzeinstellungen für ausgehende E-Mails anpassen und so besser auf individuelle Bedürfnisse einstellen.

Anpassen der Einstellungen des MailSafe-Schutzes für ausgehenden Datenverkehr:

1. Öffnen Sie E-Mail -Schutz | Grundeinstellungen.
2. Klicken Sie auf Erweitert.

Das Fenster für den erweiterten E-Mail-Schutz wird angezeigt.

Hinweis: Der E-Mail-Schutz für ausgehenden Datenverkehr muss aktiviert sein, damit Sie auf das Dialogfeld **Erweitert** zugreifen können.

3. Wählen Sie im Bereich Schutzwarnmeldung für ausgehende E-Mails anzeigen, wenn die gewünschten Einstellungen aus.

Table 0-27 Ausgehende E-Mail

Wenn zu viele E-Mail-Nachrichten gleichzeitig gesendet werden	zeigt Endpoint Security Client eine MailSafe-Schutzwarnung für ausgehenden Datenverkehr an, wenn Ihr Computer versucht, innerhalb des festgelegten Zeitintervalls mehr als die angegebene Anzahl an E-Mail-Nachrichten zu senden.
Eine Nachricht enthält zu viele Empfänger	Endpoint Security Client zeigt eine MailSafe-Schutzwarnung für ausgehenden Datenverkehr an, wenn Ihr Computer versucht, eine E-Mail-Nachricht mit mehr als der festgelegten Anzahl an Empfängern zu senden.
Sich die Adresse des Senders nicht in dieser Liste befindet.	Endpoint Security Client zeigt eine MailSafe-Schutzwarnung für ausgehenden Datenverkehr an, wenn Ihr Computer versucht, eine E-Mail-Meldung zu senden, deren Ursprungsadresse (d. h. die Adresse im Feld Von: nicht in der Liste aufgeführt wird. Damit der Client nicht alle ausgehenden E-Mail-Nachrichten sperrt, vergewissern Sie sich,

dass Ihre gültige E-Mail-Adresse in dieser Liste
vorhanden ist.

Richtlinien

Beim Anwenden von Richtlinie schützt Endpoint Security Ihr Unternehmensnetzwerk entsprechend der vom NetzwerkAdministrator erstellten SicherheitsRichtlinie. Die Durchsetzung von UnternehmensRichtlinie tritt ein, wenn der Client in einer Endpoint Security Server-Umgebung verwendet wird. Mit Endpoint Security kann Ihr Administrator die UnternehmensRichtlinien an die Benutzer der Computer im lokalen Unternehmensnetzwerk senden. Auf diese Weise können Sie sicher stellen, dass alle Rechner im Netzwerk angemessen vor möglichen Gefahren aus dem Internet geschützt sind.

Inhalt dieses Abschnitts

Richtlinie Typen	159
Grundlegendes zur Vermittlung zwischen Richtlinie	160
Anzeigen der verfügbaren Richtlinien	160
Verwenden des Bildschirms Richtlinien	160

Richtlinie Typen

Persönliche SicherheitsRichtlinie: Die Einstellungen, die Sie für Ihre Firewall, Program Control, den E-Mail-Schutz und andere Funktionen in Endpoint Security Client ausgewählt haben.

Persönliche SicherheitsRichtlinie: Einstellungen für dieselben Sicherheitsfunktionen, die allerdings vom SicherheitsAdministratorIhres Unternehmens erstellt und den Benutzern im Unternehmensnetzwerk zugewiesen wurden.

Getrennt Richtlinie: Wird von einem SicherheitsAdministratorund erzwingt bestimmte Sicherheitseinstellungen des Unternehmens, auch wenn Ihr Computer nicht mit dem Unternehmensnetzwerk verbunden ist.

Ein SicherheitsAdministrator sendet UnternehmensRichtlinien an Endpoint Security Clients im Unternehmensnetzwerk.

Wenn Ihr Computer nicht den UnternehmensRichtlinie, erzwingt Ihr Computer unter Umständen Beschränkungsregeln, die Ihren Zugriff einschränken. In diesem Fall werden Sie auf eine Webseite weitergeleitet, auf der Sie erfahren, wie Sie vorgehen müssen, damit Ihr Computer wieder den Sicherheitsrichtlinien entspricht. Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren SystemAdministrator.

Grundlegendes zur Vermittlung zwischen Richtlinie

Ihre persönliche Richtlinie ist aktiv, wenn der Client vermittelt oder keine UnternehmensRichtlinie wirksam ist. Eine UnternehmensRichtlinie kann je nach der Situation aktiviert oder deaktiviert werden.

Wenn Ihre persönliche Richtlinie und eine UnternehmensRichtlinie aktiv sind, Endpoint Security **vermittelt** zwischen den zwei Richtlinien: die einschränkendere der zwei Richtlinie wird angewendet. Wenn zum Beispiel die Sicherheit für die Internetzone durch Ihre persönliche Richtlinie auf den Wert Mittel, durch eine aktive UnternehmensRichtlinie jedoch auf den Wert Hoch gesetzt wird, wird der Wert Hoch angewendet.

Auf Grund der Vermittlung zwischen den Richtlinie kann eine aktive UnternehmensRichtlinie Datenverkehr sperren, der durch Ihre persönliche Richtlinie zugelassen ist, und umgekehrt. Wenn Endpoint Security Ihrer Meinung nach ungefährlichen Datenverkehr sperrt, wenden Sie sich an Ihren SystemAdministrator.

Anzeigen der verfügbaren Richtlinien

Je nachdem, wie Ihr Administrator Ihre Richtlinieeinstellungen konfiguriert hat, können Sie möglicherweise nur Ihre persönliche, die Unternehmens- und getrennten Richtlinien oder alle Aktualisierungen, die an Ihrer UnternehmensRichtlinie vorgenommen wurden, anzeigen.

Verwenden des Bildschirms Richtlinien

Verwenden des Bildschirms Richtlinien for Folgendes:

- Anzeigen, welche Richtlinien installiert sind, welche derzeit aktiv ist und den Zeitpunkt der letzten Aktualisierung einer Richtlinie.
- Auf eine Textversion der Einstellungen von Richtlinie für jede UnternehmensRichtlinie sowie für Ihre persönlichen Richtlinie zugreifen.

Table 0-28 Richtlinie Informationen im Bildschirm

Richtlinie Name	Name der Richtlinie. Persönliche Richtlinie: Einstellungen, die Sie für den Client über das Endpoint Security-Hauptseite festgelegt haben. Andere Namen von Richtlinie bezeichnen UnternehmensRichtlinien, die von Ihrem Administrator auf Ihrem Computer installiert wurden.
Aktiv	Diese Spalte zeigt an, ob die aufgeführte Richtlinie derzeit aktiv ist. Die persönliche Richtlinie ist stets aktiv. Der Administrator kann eine UnternehmensRichtlinie aktivieren oder deaktivieren. Wenn Ihre persönliche Richtlinie und eine andere Richtlinie aktiv sind, vermittelt Endpoint Security zwischen den zwei aktiven Richtlinien.
Letzter Serverkontakt	Bei SicherheitsRichtlinien des Unternehmens gibt diese Spalte an, wann (Datum und Uhrzeit) der Client erstmals die aktuelle Verbindung zu einem Endpoint Security Server hergestellt hat, um die aufgeführte UnternehmensRichtlinie zu erzwingen. Falls die Verbindung zum Server unterbrochen ist oder der Client eine UnternehmensRichtlinie, nicht erzwingt, wird in dieser Spalte Getrennt angezeigt.
Autor	Der Administrator der die SicherheitsRichtlinie erstellt und zugewiesen hat. Bei der persönlichen Richtlinie wird hier N/A angezeigt.
Bereich "Detailinformationen für Eintrag"	Details zur Richtlinie, die gerade in der Liste ausgewählt ist.

Warnungen und Protokolle

Sie können sich bei jeder Schutzmaßnahme des Clients eine Meldung anzeigen lassen oder nur dann, wenn der Warnung mit hoher Wahrscheinlichkeit eine bösartige Aktivität zu Grunde liegt. Sie haben zudem die Wahl, alle Warnungen, nur erstrangige Warnungen oder Warnungen, die bei einem bestimmten Netzwerkverkehrstyp auftreten, protokollieren zu lassen.

Inhalt dieses Abschnitts

Grundlegendes zu Warnungen und Protokollen	163
Einstellen grundlegender Warn- und Protokolloptionen	165
Ein- und Ausblenden von Warnungen	166
Festlegen der Ereignis- und Programmprotokollierungsoptionen	167

Grundlegendes zu Warnungen und Protokollen

Die Warn- und Protokollierfunktionen des Clients informieren Sie angemessen und rechtzeitig über die Vorgänge auf Ihrem Computer. Zudem können Sie jederzeit zurückgehen und Details zu früheren Warnungen anzeigen.

Informationen zu Warnungen

Endpoint Security Client generiert zwei Typen von Warnungen: *unternehmensbezogene* oder *persönliche*. Diese entsprechen den Einstellungen oder Regeln in der aktiven Richtlinie.

Beide Typen Richtlinie weisen drei Kategorien von Warnungen auf: *Hinweise*, *Programm-* und *Netzwerkwarnungen*.

Weitere Informationen dazu, wie Sie auf spezifische Warnungen reagieren, finden Sie unter **Warnungsmeldungen - Referenz** auf Seite [173](#).

Hinweise

Hinweise informieren Sie darüber, dass der Client eine Datenübertragung gesperrt hat, die gegen Ihre Sicherheitseinstellungen verstößt.

Hinweise erfordern keine Entscheidung Ihrerseits.

Klicken Sie auf OK, um das Meldungsfeld zu schließen.

Programmwarnungen

Bei Programmwarnungen werden Sie gefragt, ob ein Programm auf das Internet oder die Sichere Zone zugreifen darf oder eine Serverberechtigung erhält. Auf Programmwarnungen muss mit "Ja" oder "Nein" geantwortet werden. Die häufigsten Typen von Programmwarnungen sind die Warnungen **Neues Programm** und **Bekanntes Programm**.

Klicken Sie auf Ja , um dem Programm die entsprechende Berechtigung zu gewähren.

Klicken Sie auf Nein , um die Berechtigung zu verweigern.

Warnung Neues Netzwerk

Warnungen des Typs **Neues Netzwerk** werden angezeigt, wenn Sie die Verbindung zu einem Netzwerk herstellen: ein Funknetz, ein Unternehmens-LAN oder das Netzwerk Ihres Internetdiensteanbieters.

Wenn Sie an ein Heimnetzwerk oder an ein lokales Netzwerk angeschlossen sind, können Sie mit Warnungen des Typs **Neues Netzwerk** den Client sofort so konfigurieren, dass Sie Ressourcen über das Netzwerk gemeinsam nutzen können.

Informationen zur Ereignisprotokollierung

Der Client erstellt standardmäßig bei jeder Datenverkehrssperrung einen Protokolleintrag, unabhängig davon, ob eine Warnung angezeigt wird oder nicht. Protokolleinträge zeichnen die Quelle und das Ziel des Datenverkehrs, Ports, Protokolle und andere Details auf. Diese Informationen werden in einer Textdatei mit dem Namen ZALOG.txt im Internetprotokollordner gespeichert. Alle 60 Tage wird die Protokolldatei in eine datierte Datei archiviert, um den Protokollumfang so gering wie möglich zu halten.

Sie können festlegen, dass gewisse Ereigniskategorien nicht protokolliert werden. So wäre es denkbar, dass Sie nur für Firewall Protokolleinträge erstellen oder Einträge für einen bestimmten Programmwarnungstyp unterdrücken möchten.

Einstellen grundlegender Warn- und Protokolloptionen

Mit grundlegenden Warn- und Protokolloptionen können Sie den Ereignistyp festlegen, für den der Client eine Warnung anzeigt, und außerdem bestimmen, für welche Ereignisse ein Protokolleintrag erstellt wird.

Festlegen der Warnungsereignisstufe

Mit dem Steuerelement Angezeigte Warnungsereignisse in der Registerkarte Grundeinstellungen von Warnungen & Protokollen können Sie Warnungen nach Klassifizierung anzeigen. Programmwarnungen werden immer angezeigt, da Sie dadurch zur Angabe aufgefordert werden, ob Zugriffsrechte gewährt werden sollen oder nicht.

So legen Sie die Warnungsereignisstufe fest:

1. Öffnen Sie Warnungen & Protokolle | Grundeinstellungen.
2. Wählen Sie im Bereich Angezeigte Warnungsereignisse die gewünschte Einstellung aus.
 - **Hoch:** Zeigt eine Warnung für alle auftretenden Sicherheitsereignisse an, sowohl erstrangige als auch zweitrangige.
 - **Mittel:** Zeigt nur hochrangige Warnungen an, die sehr wahrscheinlich auf Hackeraktivität zurückzuführen sind.
 - **Aus:** Zeigt nur Programmwarnungen an. Hinweise werden nicht angezeigt.

Festlegen der Ereignis- und Programmprotokollierungsoptionen

In den Ereignis- und Programmprotokollierungsbereichen können Sie festlegen, welche Arten von Hinweisen und Programmwarnungen protokolliert werden sollen.

So aktivieren und deaktivieren Sie die Ereignis- und Programmprotokollierung:

1. Öffnen Sie Warnungen & Protokolle | Grundeinstellungen.
2. Wählen Sie im Bereich Ereignisprotokollierung die gewünschte Einstellung aus.

- **Ein:** Erstellt für alle Ereignisse einen Protokolleintrag.
 - **Aus:** Es werden keine Ereignisse protokolliert.
3. Wählen Sie im Bereich **Programmprotokollierung** die gewünschte Protokollierungsstufe aus.
- **Hoch:** Erstellt für alle Programmwarnungen einen Protokolleintrag.
 - **Mittel:** Erstellt nur für erstrangige Programmwarnungen einen Protokolleintrag.
 - **Aus:** Es werden keine Programmereignisse protokolliert.

Ein- und Ausblenden von Warnungen

Sie können festlegen, ob Sie bei allen Sicherheits- und Programmereignissen gewarnt werden möchten oder nur bei Ereignissen, die mit großer Wahrscheinlichkeit auf eine bösartige Aktivität zurückzuführen sind.

Ein- und Ausblenden von Firewall-Warnungen

Mit der Registerkarte **Warnungsereignisse** lassen sich Warnungsanzeigen genauer steuern. Sie können festlegen, für welche Arten von gesperrtem Datenverkehr Firewall und Programmwarnungen angezeigt werden sollen.

So zeigen Sie Firewall oder Programmwarnungen an oder blenden diese aus:

1. Öffnen Sie **Warnungen & Protokolle | Grundeinstellungen**.
2. Klicken Sie auf **Erweitert**.
Das Fenster **Warnungs&Protokolleinstellungen** wird angezeigt.
3. Öffnen Sie die Registerkarte **Warnungsereignisse**.
4. Wählen Sie in der Spalte **Warnung** die Art des gesperrten Datenverkehrs aus, für den der Client eine Warnung anzeigen soll.
5. Klicken Sie auf **Übernehmen**.

Festlegen der Ereignis- und Programmprotokollierungsoptionen

Sie können festlegen, ob der Client Sicherheits- und Programmereignisse aufzeichnet, indem Sie die Protokollierung für jeden Warnungstyp entweder aktivieren oder deaktivieren.

Format der Protokollarchivierung

Sie können die Feldtrennzeichen für Ihre Text-Protokolldateien angeben.

So formatieren Sie Protokolleinträge:

1. Öffnen Sie Warnungen & Protokolle.
2. Klicken Sie auf Erweitert.

Das Fenster Erweiterte Meldungen und Protokolleinstellungen wird angezeigt.

3. Öffnen Sie die Registerkarte Protokolleinstellungen.
4. Wählen Sie im Bereich Format der Protokollarchivierung das Format aus, das für Protokolle verwendet werden soll: Tab, Komma oder Semikolon.

Anpassen der Ereignisprotokollierung

Der Client erstellt standardmäßig einen Protokolleintrag, wenn ein erstrangiges Firewallereignis auftritt. Sie können die Protokollierung von Firewallmeldungen anpassen, indem Sie Protokolleinträge für bestimmte Sicherheitsereignisse wie MailSafe abgeschirmte Anhänge, gesperrte Nicht-ISP-Pakete oder Sperrverletzungen unterdrücken oder zulassen.

So erstellen oder unterdrücken Sie Protokolleinträge nach Ereignistyp:

1. Öffnen Sie Warnungen & Protokolle | Grundeinstellungen.
2. Klicken Sie auf Erweitert.

Das Fenster Erweiterte Meldungen und Protokolleinstellungen wird angezeigt.

3. Wählen Sie Warnungsereignisse aus.
4. Wählen Sie in der Spalte Protokoll den Ereignistyp aus, für den der Client einen Protokolleintrag erstellen soll.

5. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.
6. Klicken Sie auf **OK**, um das Fenster & Erweiterte Warnmeldungen und Protokolleinstellungen zu schließen.

Anpassen der Programmprotokollierung

Der Client erstellt standardmäßig einen Protokolleintrag, wenn eine Programmwarnung auftritt. Sie können die Protokollierung von Programmwarnungen anpassen, indem Sie Protokolleinträge für bestimmte Programmwarnungsarten, wie z.B. Warnungen bei bekannten Programmen oder Serverprogrammwarnungen unterdrücken oder zulassen.

So erstellen oder unterdrücken Sie Protokolleinträge nach Ereignistyp:

1. Öffnen Sie **Warnungen & Protokolle | Grundeinstellungen**.
2. Klicken Sie im Bereich **Programmprotokollierung** auf **Benutzerdefiniert**.
3. Wählen Sie in der Spalte **Programmprotokolle** den Ereignistyp aus, für den der Client einen Protokolleintrag erstellen soll.
4. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.
5. Klicken Sie auf **OK**, um das Fenster & Erweiterte Warnmeldungen und Protokolleinstellungen zu schließen.

Anzeigen von Protokolleinträgen

Sie können Protokolleinträge in einer Textdatei mit einem Texteditor oder in der Protokollanzeige anzeigen. Die allgemeinen Informationen im Protokoll sind gleich, obwohl das Format leicht voneinander abweicht.

So zeigen Sie das aktuelle Protokoll in der Protokollanzeige an:

1. Öffnen Sie **Warnungen & Protokolle | Protokollanzeige**.
2. Wählen Sie die Anzahl der Warnungen (von 1 bis 99) aus, die in der Warnungsliste angezeigt werden soll.

Sie können die Liste nach einem beliebigen Feld sortieren, indem Sie auf die jeweilige Spaltenüberschrift klicken.

3. Klicken Sie auf einen Protokolleintrag, um Protokolleintragsdetails anzuzeigen.

Protokollanzeigefelder

In der Dropdown-Liste **Warnmeldungstyp** oben im Bildschirm Protokollanzeige, können Sie Programm-, Firewall, Antivirus, Anti-Spyware und SmartDefense-Warnmeldungen anzeigen.

Table 0-29 Informationen der Protokollanzeige

Spaltenüberschrift	Beschreibung
Klassifizierung	Jede Warnung wird als „Kritisch“, „Hoch“ oder „Mittel“ eingestuft. Warnungen, denen mit hoher Wahrscheinlichkeit ein Hackerangriff zu Grunde liegt, werden als „Kritisch“ oder „Hoch“ eingestuft. Warnungen, deren Ursache mit hoher Wahrscheinlichkeit auf unbeabsichtigten, aber harmlosen Netzwerkverkehr zurückzuführen ist, werden als "Mittel" eingestuft.
Datum / Uhrzeit	Datum und Uhrzeit der Warnung.
Typ	Warnungstyp: Firewall, Programm, Erkennung von gefährlichem Code, aktivierte Sperre, Scan, Aktualisierung oder Behandlung.
Protokoll	Wählen Sie in der Dropdown-Liste Warnmeldungstyp die Option Firewall aus, um die Spalte Protokoll anzuzeigen. Identifiziert das Protokoll, das von dem Datenverkehr verwendet wurde, der die Warnung ausgelöst hat.
Programm	Der Name des Programms, das versucht, Daten zu senden oder zu empfangen (nur bei Programmwarnungen).
Quell-IP-Adresse	Die IP-Adresse des Computers, der die vom Client gesperrten Daten gesendet hat.
Ziel-IP-Adresse	Die IP-Adresse des Computers, an den die gesperrten Daten gesendet wurden.
Richtung	Die Richtung des gesperrten Datenverkehrs: Eingehend oder Ausgehend beim/vom Computer.
Maßnahme	Vom Client durchgeführte Verarbeitung des Datenverkehrs.
Anzahl	Anzahl der Warnungen gleichen Typs, mit gleicher Quelle, gleichem Ziel und gleichem Protokoll, die während einer Sitzung aufgetreten sind.

Spaltenüberschrift	Beschreibung
Quell-DNS	Der Domänenname des Computers, der die Daten gesendet hat, welche die Warnung ausgelöst haben.
Ziel-DNS	Der Domänenname des Computers, der die Daten empfangen sollte, welche die Warnung ausgelöst haben.
Richtlinie	Der Name der Richtlinie mit der Sicherheitseinstellung oder Regel, die die Warnung ausgelöst hat. Endpoint Security Client erkennt drei Richtlinientypen: persönliche , unternehmensweite und getrennte Richtlinien.
Regel	Wählen Sie in der Dropdown-Liste Warnmeldungstyp die Option Firewall aus, um die Spalte Regel anzuzeigen. Wenn eine Warnung durch die in einer klassischen Firewallregel festgelegten Bedingungen verursacht wurde, enthält diese Spalte den Namen der Regel.

Anzeigen des Textprotokolls

Von der Endpoint Security ausgegebene Warnungen werden standardmäßig in der Datei `\WINDIR\Internet Logs\ZAlog.txt` protokolliert (wobei *WINDIR* normalerweise `c:\Windows` ist).

So zeigen Sie das aktuelle Protokoll als Textdatei an:

1. Öffnen Sie **Warnungen & Protokolle | Grundeinstellungen**.
2. Klicken Sie auf **Erweitert**.

Das Fenster **& Erweiterte Warnmeldungen und Protokolleinstellungen** wird geöffnet.
3. Öffnen Sie die Registerkarte **Protokolleinstellungen**.
4. Klicken Sie im Bereich **Protokollarchiv-Speicherort** auf die Schaltfläche **Protokoll anzeigen**.

Table 0-30 Informationen des Textprotokolls

Feld	Beschreibung	Beispiel
Typ	Der Typ des aufgezeichneten Ereignisses.	FWIN
Datum	Das Datum der Warnung im Format JJJJ/MM/TT.	2001/12/31 (31. Dezember 2001)
Zeit	Die lokale Uhrzeit der Warnung. In diesem Feld wird zudem die Differenz zwischen der Ortszeit und der Greenwich Mean Time (GMT) in Stunden angezeigt.	17:48:00 -8:00GMT (17:48 minus acht Stunden von Greenwich Mean Time; als GMT ausgedrückt wäre die Uhrzeit dann 01:48.)
Quelle	Die IP-Adresse des Computers, der das gesperrte Paket gesendet hat, und der verwendete Port ODER das Programm auf Ihrem Computer, das die Zugriffsrechte angefordert hat.	192.168.1.1:7138 (Firewallereignisse) Microsoft Outlook
Ziel	Die IP-Adresse und Portnummer des Computers, an den das gesperrte Paket adressiert war.	192.168.1.101:0
Transport	Das verwendete Protokoll (Pakettyp).	UDP

Archivieren von Protokolleinträgen

In regelmäßigen Intervallen erfolgt eine Archivierung des Inhalts der Datei `ZALog.txt` in einer Datei mit Datumsstempel (z.B. `ZALog2005.09.12.txt` für den 12.09.05). So bleibt die Dateigröße in überschaubaren Dimensionen.

Verwenden Sie Windows-Explorer, um zum Verzeichnis der archivierten Protokolldateien zu navigieren.

So legen Sie die Archivierungshäufigkeit fest:

1. Öffnen Sie Warnungen & Protokolle | Grundeinstellungen.

2. Klicken Sie auf **Erweitert**.
3. Öffnen Sie die Registerkarte **Protokolleinstellungen**.
4. Aktivieren Sie das Kontrollkästchen **Intervall der Protokollarchivierung**.
Wenn dieses Kontrollkästchen nicht markiert ist, zeichnet Endpoint Security weiterhin Ereignisse zur Anzeige auf der Registerkarte **Protokollanzeige** auf, archiviert diese Ereignisse jedoch nicht in der Datei **ZALog.txt**.
5. Geben Sie im **Protokollintervallbereich** das **Protokollintervall** (zwischen 1 und 60 Tagen) an.

Verwenden von SmartDefense Advisor

Der Check Point von Check Point ist ein Online-Dienstprogramm, mit dem Sie eine Warnung auf ihre möglichen Ursachen hin untersuchen können. Dies ist hilfreich bei der Entscheidung, wie auf eine Programmwarnung reagiert werden soll.

Klicken Sie in einem Popup-Fenster der Warnungsmeldung auf die Schaltfläche **Mehr Info**, um den SmartDefense Advisor aufzurufen, sofern verfügbar.

Endpoint Security leitet daraufhin Informationen zur Warnung an den SmartDefense Advisor weiter. Sie erhalten vom SmartDefense Advisor einen Artikel, in dem die Warnung erklärt wird und Sie ggf. darüber informiert werden, was zu tun ist, um Ihre Sicherheit weiterhin zu gewährleisten.

So leiten Sie Warnungen an den SmartDefense Advisor weiter:

1. Öffnen Sie **Warnungen & Protokolle | Protokollanzeige**.
2. Klicken Sie mit der rechten Maustaste in den **Warnungsdatensatz**, den Sie weiterleiten möchten, und wählen Sie **Mehr Info** aus.

Warnungsmeldungen - Referenz

Bei Verwendung von Endpoint Security können verschiedene Arten von Warnungen angezeigt werden. In dieser Referenz erfahren Sie, warum Warnungen auftreten, was sie bedeuten, und wie Sie jeweils vorgehen.

Inhalt dieses Abschnitts

Hinweise	173
Programmwarnungen	178

Hinweise

Hinweise informieren Sie darüber, dass der Client eine Datenübertragung gesperrt hat, die gegen Ihre Sicherheitseinstellungen verstößt.

Hinweise erfordern keine Entscheidung Ihrerseits.

Klicken Sie auf OK, um das Meldungsfeld zu schließen.

Firewallmeldung/Geschützt

Firewallmeldungen gehören zu den am häufigsten angezeigten Hinweisen.

Firewallmeldungen informieren Sie darüber, dass die Endpoint Security Firewall den Datenverkehr auf Grund der Einschränkungen für Ports und Protokolle oder auf Grund anderer Firewallregeln gesperrt hat.

Gründe für das Auftreten von Firewallmeldungen

Bei erstrangigen Firewallmeldungen ist der obere Bereich der Warnung rot markiert. Erstrangige Warnungen sind oft auf eine bösartige Aktivität zurückzuführen.

Bei zweitrangigen Firewallmeldungen ist der obere Bereich der Warnung orange markiert. Zweitrangige Firewallmeldungen werden oft durch harmlosen Netzwerkverkehr verursacht, Beispielsweise wenn Ihr Internetdienstanbieter mit Hilfe der Ping-Funktion die Verbindung überprüft. Sie können jedoch auch dadurch verursacht werden, dass ein Hacker versucht, ungeschützte Ports auf Ihrem Computer zu ermitteln.

Erforderliche Schritte

Wenn es sich um ein Heimnetzwerk oder Unternehmensnetzwerk handelt und die Sicherheitsstufe der Sicherer Zone auf HOCH gesetzt ist, kann auch normaler LAN-Verkehr (z. B. NetBIOS-Übertragungen) Firewallmeldungen auslösen. Setzen Sie daher die Sicherheitsstufe der Sicherer Zone auf MITTEL.

Die Endpoint Security zeigt standardmäßig ausschließlich erstrangige Firewallmeldungen an. Wenn Sie die Standardeinstellung geändert haben, werden unter Umständen viele zweitrangige Meldungen angezeigt. Setzen Sie daher die Einstellungen für die Anzeige von Warnungen auf MITTEL.

Wenn Sie in einem Heimnetzwerk oder Unternehmens-LAN sehr viele Firewallmeldungen erhalten, kann es zu einer Beeinträchtigung der Netzwerkkommunikation kommen. In einem solchen Fall können Sie die Warnungen vermeiden, indem Sie Ihr Netzwerk der Sicherer Zone hinzufügen.

Das Auftreten von Firewallmeldungen verringern.

Wiederholte Warnungen können darauf hindeuten, dass eine sichere Ressource mehrmals versucht hat, eine Verbindung zu Ihrem Computer herzustellen. Falls Sie häufig Firewallmeldungen erhalten, die vermutlich nicht durch Angriffe verursacht werden, können Sie das Problem auf folgende Weise beheben:

- Ermitteln Sie die Vertrauenswürdigkeit der Quelle der Warnungen.
- Leiten Sie wiederholte Warnungen an den SmartDefense Advisor weiter, um die Quell-IP-Adresse, welche die Warnungen verursacht hat, zu ermitteln.
- Wenn die Warnungen von einer Quelle verursacht wurden, der Sie vertrauen möchten, fügen Sie diese der Sicherer Zone hinzu.
- Ermitteln Sie, ob Ihr Internetdienstanbieter Ihnen Heartbeat-Signale sendet.

- Führen Sie die empfohlenen Verfahren zur Handhabung eines ISP-Heartbeat aus. Siehe **Zulassen von ISP Heartbeat-Signalen** siehe "[Zulassen von ISP-Heartbeat-Signalen](#)" auf Seite 194.

MailSafemeldung

MailSafe-Warnungen informieren Sie darüber, dass Endpoint Security eine möglicherweise gefährliche ausgehende E-Mail-Nachricht unter Quarantäne gestellt hat.

Gründe für das Auftreten von MailSafemeldungen

Wenn eine Verletzung der MailSafe-Schutzeinstellungen für ausgehenden Datenverkehr erfolgt, wie zum Beispiel eine E-Mail mit zu vielen Empfängern oder zu viele E-Mails in einer zu kurzen Zeitspanne, kann eine MailSafe-Warnung auftreten.

Erforderliche Schritte

- Untersuchen Sie die Warnung sorgfältig. Stimmt die beschriebene Aktivität mit Aktionen überein, die Sie vor Kurzem durchgeführt haben? Haben Sie beispielsweise kürzlich versucht, eine seriöse E-Mail an viele Empfänger zu senden, oder haben Sie viele E-Mails in einem kurzen Zeitraum gesendet? Falls eine dieser Aktionen auf Sie zutrifft, können Sie die MailSafe-Einstellungen für ausgehenden Datenverkehr anpassen, so dass sie besser Ihren Anforderungen entsprechen. Siehe **Schutz für MailSafe ausgehenden Datenverkehr** siehe "[Schutz für ausgehenden MailSafeverkehr](#)" auf Seite 155.
- Stellen Sie sicher, dass Ihre E-Mail-Adresse sich in der Liste der genehmigten Absender befindet. Wenn Sie die Option **Wenn sich die Adresse des Absenders nicht in dieser Liste befindet** ausgewählt haben und Ihre E-Mail-Adresse sich nicht auf dieser Liste befindet oder falsch buchstabiert ist, fügen Sie Ihre gültige E-Mail-Adresse dieser Liste hinzu.

Warnungen bei gesperrtem Programm

Warnungen bei gesperrten Programmen informieren Sie darüber, dass Endpoint Security es einer Anwendung auf Ihrem Computer nicht gestattet hat, auf Ressourcen der Internetzone oder der Sicheren Zone zuzugreifen. Durch Klicken auf OK gestatten Sie dem Programm den Zugriff nicht, sondern bestätigen lediglich, dass Sie die Warnung zur Kenntnis genommen haben.

Bedeutung von Warnungen bei gesperrtem Programm

Warnungen bei gesperrten Programmen treten auf, wenn ein Programm versucht, auf die Internetzone oder die Sichere Zone zuzugreifen, obwohl Sie dies dem Programm ausdrücklich verweigert haben.

Erforderliche Schritte

Wenn Sie dem gesperrten Programm Zugriff auf die Internetzone oder die Sichere Zone gewähren möchten, öffnen Sie die Registerkarte Programme und erteilen dem Programm Zugriffsrechte.

Reduzieren der Anzahl von Warnungen bei gesperrtem Programm

Gehen Sie wie folgt vor, wenn Sie Warnungen bei gesperrten Programmen deaktivieren möchten:

- Wenn eine Warnung bei gesperrtem Programm angezeigt wird, wählen Sie die Option **Dieses Dialogfeld nicht erneut anzeigen** aus, und klicken Sie danach auf OK. Von nun an werden alle Warnungen bei gesperrten Programmen ausgeblendet. Beachten Sie, dass dadurch die Warnungen bei neuen Programmen, bekannten Programmen oder Serverprogrammwarnungen nicht beeinflusst werden.
- Klicken Sie im Bildschirm Program Control auf **Erweitert**, um auf die Registerkarte & Warnungen und Funktionen zuzugreifen. Deaktivieren Sie dann das Kontrollkästchen **Bei verweigertem Internetzugriff Meldung anzeigen**.



Hinweis - Wenn Sie Warnungen bei gesperrten Programmen deaktivieren, wird die Sicherheitsstufe nicht beeinträchtigt.

Meldungen für Internetsperre

Meldungen für die Internetsperre zeigen an, dass Endpoint Security eingehenden oder ausgehenden Datenverkehr gesperrt hat, weil die Internetsperre aktiviert wurde. Durch Klicken auf OK heben Sie die Sperre nicht auf, sondern bestätigen lediglich, dass Sie die Warnung zur Kenntnis genommen haben.

Bedeutung von Meldungen für Internetsperre

Diese Warnungen treten nur auf, wenn die Internetsperre aktiviert wurde.

Reduzieren der Anzahl von Meldungen für Internetsperre

Wenn Meldungen für die Internetsperre häufig auftreten, wird dies möglicherweise dadurch verursacht, dass die Internetsperre durch die Einstellung Automatische Internetsperre nach kurzer Inaktivität aktiviert wird.

Gehen Sie wie folgt vor, damit die Warnungen weniger häufig angezeigt werden:

- Deaktivieren Sie die automatische Internetsperre.
- Erhöhen Sie das Inaktivitätsintervall, nach dessen Ablauf die automatische Internetsperre aktiviert wird (siehe **Aktivieren der automatischen Sperre** auf Seite [100](#)).

Einhaltungswarnungen

Einhaltungswarnungen treten auf, wenn Endpoint Security Server in Verbindung mit Endpoint Security Client feststellt, dass Ihr Computer die Sicherheitsanforderungen des Unternehmens nicht erfüllt. Je nach Art der Nichterfüllung ist Ihr Zugriff auf das Unternehmensnetzwerk eventuell *eingeschränkt* oder sogar *unmöglich*.

Bedeutung von Einhaltungswarnungen

Diese Warnungen werden angezeigt, wenn Sie versuchen, eine Verbindung zu Ihrem Unternehmensnetzwerk herzustellen und dabei die Richtlinie nicht eingehalten wird, die in Endpoint Security Server gespeichert ist.

Erforderliche Schritte

Zusammen mit bestimmten Webseiten enthalten Einhaltungswarnungen Informationen zu den Maßnahmen, die Sie ergreifen müssen, um die Einstellungen gemäß den SicherheitsRichtlinie vorzunehmen.

- Wenn das Problem nicht sofort behoben werden muss, ist Ihr Zugriff auf das Unternehmensnetzwerk möglicherweise *eingeschränkt*. Sie können weiterhin auf einige Ressourcen im Unternehmensnetzwerk zugreifen, jedoch sollten Sie schnellstmöglich die notwendigen Schritte durchführen, um Ihren Computer an die Anforderungen anzupassen.
- Wenn das Problem sofort behoben werden muss, ist der Zugriff auf das Unternehmensnetzwerk eventuell *unmöglich*. In diesem Fall können Sie nur auf die Webseite zugreifen, die Anweisungen dazu enthält, wie Sie Ihren

Computer an die Sicherheitsanforderungen des Unternehmens anpassen können.

Klicken Sie auf den Link in der Warnung oder auf der entsprechenden Webseite, und beginnen Sie mit den erforderlichen Maßnahmen. Dazu gehört normalerweise die Installation einer neueren Version von Endpoint Security oder einer anerkannten Antivirus-Software. Wenn Sie eine Einhaltungswarnung erhalten und nicht sicher sind, wie Sie Ihren Computer an die Sicherheitsanforderungen des Unternehmens anpassen können, wenden Sie sich an Ihren SystemAdministrator.

Ihr Administrator hat die Möglichkeit, Endpoint Security so zu konfigurieren, dass automatisch alle Anwendungen installiert werden, die notwendig sind, damit Ihr Computer die Unternehmensrichtlinien erfüllt. Dies kann in bestimmten Fällen dazu führen, dass ein Programm ohne Warnung auf Ihrem Computer installiert und ein Neustart Ihres Computers erforderlich wird. Wenn Ihr System automatisch neu gestartet wird oder wenn ein Programm versucht, sich auf Ihrem Computer zu installieren, wenden Sie sich an Ihren SystemAdministrator.

Reduzieren der Anzahl von Einhaltungswarnungen

Sie können die Anzeige von Einhaltungswarnungen vermeiden, indem Sie stets dafür sorgen, dass Ihr Computer die Sicherheitsrichtlinie einhält, die von Ihrem Administrator festgelegt sind.

Programmwarnungen

Programmwarnungen werden meistens bei aktiver Verwendung eines Programms angezeigt. Haben Sie beispielsweise die Endpoint Security soeben installiert und öffnen zum Versenden einer E-Mail unmittelbar darauf Microsoft Outlook, werden Sie in einer Programmwarnung gefragt, ob Sie zulassen möchten, dass Outlook auf das Internet zugreift. Programmwarnungen können jedoch auch auftreten, wenn ein Trojaner oder Wurm auf Ihrem Computer versucht, sich weiter zu versenden.

Warnung „Neues Programm“

Über die Warnung "Neues Programm" können Sie Programmen Zugriffsrechte gewähren, die bisher noch keinen Zugriff auf die Internetzone oder die Sichere Zone angefordert haben.

Klicken Sie auf **Ja**, um dem Programm Zugriff zu gewähren.

Klicken Sie auf **Nein**, um dem Programm den Zugriff zu verweigern.

Bedeutung der Warnung „Neues Programm“

Die Warnung "Neues Programm" wird angezeigt, wenn ein Programm ohne Zugriffsrechte versucht, eine Verbindung zu einem Computer in der Internetzone oder der Sicheren Zone herzustellen.

Nach der Installation der Endpoint Security wird wahrscheinlich mehrmals die Warnung Neues Programm angezeigt.

Erforderliche Schritte

Klicken Sie im Popup-Fenster der Warnung als Antwort auf die folgenden Fragen auf Ja oder Nein:

- Haben Sie soeben ein Programm gestartet, das zur ordnungsgemäßen Funktion diese Berechtigung erfordert? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit unbedenklich, auf Ja zu klicken. Trifft dies nicht zu, fahren Sie mit dem nächsten Schritt fort.
- Erkennen Sie den im Warnungsfenster angezeigten Programmnamen? Falls ja, benötigt das Programm für seine Funktion diese Berechtigung? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit unbedenklich, auf Ja zu klicken. Trifft dies nicht zu, oder sind Sie sich nicht sicher, fahren Sie mit dem nächsten Schritt fort.
- Wenn Sie sich in Ihrer Entscheidung unsicher fühlen, sollten Sie auf Nein klicken. Eine Berechtigung kann einem Programm auch zu einem späteren Zeitpunkt über die Registerkarte Programme erteilt werden.

Reduzieren der Anzahl von Warnungen des Typs „Neues Programm“

Kurz nach der Installation von Endpoint Security werden Sie möglicherweise mehrere Warnungen des Typs Neues Programm erhalten. Sobald Sie allen neuen Programmen Zugriffsrechte zugewiesen haben, erhalten Sie diese Warnungen nur noch selten.

Aktivieren Sie die Option Diese Einstellung beim nächsten Start des Programms verwenden, um Warnungen vom Typ Bekanntes Programm zu unterbinden.

Warnung „Bekanntes Programm“

Warnungen bei bekannten Programmen werden angezeigt, wenn ein Programm, dem bei der letzten Anfrage keine Zugriffsrechte erteilt wurden, versucht, eine

Verbindung zu einem Computer in der Internetzone oder der Sicheren Zone aufzubauen.

Bedeutung der Warnung „Bekanntes Programm“

Wenn Sie eine Warnung des Typs Neues Programm mit Ja oder Nein beantworten und dabei nicht **Diese Einstellung beim nächsten Start des Programms verwenden** aktiviert haben, erhalten Sie bei der nächsten Anfrage des Programms nach Zugriffsrechten eine Warnung des Typs Bekanntes Programm.

Erforderliche Schritte

Reagieren Sie auf Warnungen bei bekannten Programmen genauso wie auf Warnungen bei neuen Programmen.

Über die Warnung "Neues Programm" können Sie Programmen Zugriffsrechte gewähren, die bisher noch keinen Zugriff auf die Internetzone oder die Sichere Zone angefordert haben.

Klicken Sie auf Ja, um dem Programm Zugriff zu gewähren.

Klicken Sie auf Nein, um dem Programm den Zugriff zu verweigern.

Reduzieren der Anzahl von Warnungen des Typs „Bekanntes Programm“

Aktivieren Sie die Option **Diese Einstellung beim nächsten Start des Programms verwenden**, bevor Sie in einem Warnungsfenster für ein neues oder bekanntes Programm auf Ja oder Nein klicken. Dadurch wird auf der Registerkarte Programme für die Berechtigung des Programms entweder Zulassen oder Sperren festgelegt.

Warnung „Geändertes Programm“

Warnungen bei geänderten Programmen signalisieren, dass sich ein Programm, das zuvor Zugriffsrechte oder Serverberechtigungen angefordert hat, geändert hat.

Klicken Sie auf Ja, um dem geänderten Programm Zugriff zu gewähren. Klicken Sie auf Nein, um dem Programm den Zugriff zu verweigern.

Bedeutung der Warnung „Geändertes Programm“

Einige Programme sind so konfiguriert, dass sie regelmäßig auf das Internet zugreifen, um nach verfügbaren Aktualisierungen zu suchen. Warnungen bei

geänderten Programmen können auftreten, wenn ein Programm seit dem letzten Zugriff auf das Internet aktualisiert wurde. Sie können jedoch auch dann auftreten, wenn ein Hacker ein Programm manipuliert hat.

Ob Programme über eine solche automatische Aktualisierungsfunktion verfügen, können Sie der Dokumentation zu Ihren Programmen oder den Support-Websites der Programmlieferanten entnehmen.

Erforderliche Schritte

Entscheiden Sie im Falle einer Warnung zu einem geänderten Programm anhand der folgenden Fragen über Ihr weiteres Vorgehen:

- Haben Sie (oder der SystemAdministrator) kürzlich das Programm aktualisiert, das nun eine Berechtigung anfordert?
 - Benötigt das Programm für seine Funktion diese Berechtigung?
- Wenn Sie beide Fragen mit „Ja“ beantworten können, ist es mit hoher Wahrscheinlichkeit unbedenklich, im Dialogfeld auf Ja zu klicken.



Hinweis - Falls Sie sich nicht sicher sind, antworten Sie mit Nein. Eine Berechtigung kann einem Programm auch später noch über die Registerkarte Programme erteilt werden.

Reduzieren der Anzahl von Warnungen des Typs „Geändertes Programm“

Warnungen zu geänderten Programmen werden immer angezeigt, da Sie darauf antworten müssen. Falls Sie ein Programm verwenden, dessen Prüfsumme sich oft ändert, können Sie die Anzeige von vielen Warnungen vermeiden, indem Sie Endpoint Security so konfigurieren, dass nur der Dateiname des Programms überprüft wird. ***Hinzufügen eines Programms zur Programmliste***“ siehe ["Hinzufügen von Programmen zur Programmliste"](#) auf Seite 104.

Warnung „Programmkomponente“

Mit der Warnung für Programmkomponenten können Sie Programmen, die noch nicht von der Endpoint Security gesicherte Komponenten verwenden, Zugang zum Internet gewähren oder verweigern. Damit erhöhen Sie den Schutz vor Hackern, die über geänderte oder gefälschte Komponenten Ihre Einschränkungen bei Program Control umgehen möchten.

Klicken Sie auf **Ja**, um einem Programm, das neue oder geänderte Komponenten verwendet, Zugang zum Internet zu gewähren.

Klicken Sie auf **Nein**, um dem Programm den Zugang zum Internet zu verweigern, solange diese Komponenten verwendet werden.

Bedeutung der Warnung „Programmkomponente“

Warnungen für Programmkomponenten werden bei einem Zugriff auf das Internet oder ein lokales Netzwerk durch ein Programm mit einzelnen Komponenten angezeigt, die noch nicht von der Endpoint Security gesichert wurden oder nach der Sicherung geändert wurden.

Endpoint Security sichert Komponenten automatisch, wenn diese zum Zeitpunkt der Freigabe eines Programms von dem Programm verwendet werden. So wird die Anzeige einer Warnung für jede einzelne von Ihrem Browser verwendete Komponente vermieden. Weitere Informationen dazu, wie die Endpoint Security Programmkomponenten sichert, finden Sie unter **Programmauthentifizierung** auf Seite [98](#).

Erforderliche Schritte

Die richtige Reaktion auf Warnungen für Programmkomponenten ist situationsabhängig. Die folgenden Fragen können Ihnen bei der Entscheidung helfen:

- Trifft eine der folgenden Aussagen zu?
- Sie haben Endpoint Security soeben erst installiert oder erneut installiert.
- Sie die Anwendung, für deren Komponente Sie die Warnung erhalten haben, erst kürzlich aktualisiert. (Der Name der entsprechenden Anwendung wird im Fenster der Warnung unter **Technische Informationen** angezeigt.)
- Die Anwendung, für deren Komponente Sie eine Warnung erhalten haben, verfügt über eine automatische Aktualisierungsfunktion.
- Eine andere Person (z.B. ein SystemAdministrator in Ihrem Unternehmen) hat ein Programm auf Ihrem Computer ohne Ihr Wissen aktualisiert.
- Führen Sie die Anwendung, für deren Komponente Sie eine Warnung erhalten haben, gerade aus?

Wenn Sie diese Fragen mit Ja beantworten können, wurden von Endpoint Security wahrscheinlich vertrauenswürdige Komponenten erkannt, die von Ihrem Browser oder einer anderen Anwendung benötigt werden. Die Warnung für

Programmkomponenten kann in der Regel ohne Sicherheitsbedenken mit **Ja** beantwortet werden.

Klicken Sie auf **Ja**, um einem Programm, das neue oder geänderte Komponenten verwendet, Zugang zum Internet zu gewähren. Können Sie die Fragen nicht mit **Ja** beantworten oder erscheint Ihnen eine Komponente als verdächtig, ist es sicherer, die Warnung mit **Nein** zu beantworten.

Klicken Sie auf **Nein**, um dem Programm den Zugang zum Internet zu verweigern, solange diese Komponenten verwendet werden.



Hinweis - Fühlen Sie sich in Ihrer Entscheidung unsicher, oder möchten Sie die Komponente durch Klicken auf **Nein** ablehnen, können Sie diese noch eingehend auf Sicherheit überprüfen.

Reduzieren der Anzahl von Warnungen des Typs „Programmkomponente“

Wenn Sie kurz nach der Installation der Endpoint Security die Einstellung der Programmauthentifizierungsstufe auf **Hoch** setzen, so werden Sie mit einer Vielzahl von Warnungen für Programmkomponenten konfrontiert. Bei der Einstellung der Authentifizierungsstufe auf **Hoch** kann die Endpoint Security die zahlreichen Programmbibliotheken (DLLs) und sonstige vom Browser und anderen Anwendungen regelmäßig verwendeten Komponenten nicht automatisch sichern.

Setzen Sie für die ersten zwei Tage nach der Installation der Endpoint Security die Authentifizierungsstufe auf **Mittel**, um die Anzahl der angezeigten Warnungen zu reduzieren.

Nach einigen Tagen werden Sie von der Endpoint Security nur noch selten viele Programmwarnungen erhalten.

Warnung „Serverprogramm“

Mit Hilfe von Serverprogrammwarnungen können Sie einem Programm auf Ihrem Computer Serverberechtigungen erteilen.

Bedeutung der Warnung „Serverprogramm“

Serverprogrammwarnungen werden angezeigt, wenn ein Programm auf Ihrem Computer Serverberechtigungen für die Internetzone oder die Sichere Zone anfordert, das noch keine Serverberechtigungen erhalten hat.

Serverberechtigungen sind nur für sehr wenige Programme erforderlich. Nachfolgend finden Sie einige gängige Programme, die Serverberechtigungen benötigen:

- Chat
- Internet-Anklopffunktion
- Musik-Filesharing (z.B. Napster)
- Streaming Media (z.B. RealPlayer)
- Voice over Internet (Voice over IP, VoIP)
- Web-Meeting

Wenn Sie Programme des oben beschriebenen Typs verwenden, die Serverberechtigungen benötigen, um ordnungsgemäß zu funktionieren, erteilen Sie dem Programm Serverberechtigungen, bevor Sie mit dem Programm arbeiten.

Siehe **Erteilen der Serverberechtigung** siehe "[Erteilen der Serverberechtigung für Programme](#)" auf Seite 106.



Hinweis - Falls Ihr Browser keine Berechtigung zum Zugriff auf das Internet hat, werden Sie an die Online-Hilfe weitergeleitet.

Erteilen Sie Ihrem Browser Zugriffsrechte für das Internet, um auf den SmartDefense Advisor zugreifen zu können. Siehe **Gewähren von Internet-Zugriffsrechten für Programme** auf Seite 105.

Erforderliche Schritte

Bevor Sie auf die Serverprogrammwarnung reagieren, sollten Sie sich folgende Fragen stellen:

- Haben Sie soeben ein Programm gestartet, das zur ordnungsgemäßen Funktion diese Berechtigung erfordert? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit für die Sicherheit unbedenklich, die Warnung mit „Ja“ zu beantworten. Trifft dies nicht zu, fahren Sie mit dem nächsten Schritt fort.
- Erkennen Sie den Namen des Programms im Warnungsfenster? Wenn ja, halten Sie es für möglich, dass dieses Programm Zugriffsrechte benötigt? Trifft dies zu, ist es mit hoher Wahrscheinlichkeit für die Sicherheit unbedenklich, die Warnung mit „Ja“ zu beantworten.
- Klicken Sie im Warnungsfenster auf die Schaltfläche **Mehr Info**. Die Informationen der Warnung (z.B. der Name des Programms und die Adresse, zu der eine Verbindung hergestellt werden sollte) werden an den SmartDefense Advisor weitergeleitet, und es wird eine Webseite mit weiteren Informationen zur Warnung und zum betroffenen Programm angezeigt. Entscheiden Sie an

Hand der Informationen aus dem SmartDefense Advisor, ob eine Bestätigung der Warnung mit **Ja** unbedenklich ist. Siehe **Verwenden von SmartDefense Advisor** auf Seite [172](#).

- Falls Sie sich immer noch nicht sicher sind, ob es sich um ein vertrauenswürdiges Programm handelt oder ob das Programm eine Serverberechtigung benötigt, klicken Sie auf **Nein**. Falls erforderlich, können Sie dem Programm zu einem späteren Zeitpunkt immer noch über die Registerkarte Programme Serverberechtigung gewähren. Siehe **Erteilen der Serverberechtigung für Programme** auf Seite [106](#).

Reduzieren der Anzahl von Warnungen des Typs „Serverprogramm“

Wenn Sie Programme des oben beschriebenen Typs verwenden, die Serverberechtigungen benötigen, um ordnungsgemäß zu funktionieren, können Sie dem Programm über die Registerkarte Programme der Endpoint Security Serverberechtigungen erteilen, bevor Sie mit dem Programm arbeiten.

Erweiterte Programmwarnungen

Erweiterte Programmwarnungen sind anderen Programmwarnungen ("Neues Programm", "Bekanntes Programm" und "Geändertes Programm") ähnlich, denn sie informieren Sie darüber, dass ein Programm versucht, auf das Netzwerk zuzugreifen.

Der Unterschied besteht jedoch darin, dass das Programm versucht, den Zugriff auf das Internet über ein anderes Programm zu erhalten oder die Funktionen eines anderen Programms zu manipulieren.

Bedeutung der Programmwarnungen

Erweiterte Programmwarnungen treten in zwei verschiedenen Situationen auf: Wenn ein Programm versucht, durch eine Anweisung an ein anderes Programm eine Verbindung zu einem Computer in der Internetzone oder der Sicheren Zone herzustellen, oder wenn ein Programm versucht, durch Aufrufen der OpenProcess-Funktion die Vorgänge eines anderen Programms zu missbrauchen.

Allerdings ist der Zugriff auf ein anderes Programm bei einigen zum Betriebssystem gehörenden Programmen vorgesehen und gerechtfertigt. Wenn Sie z.B. den Windows Task-Manager zum Herunterfahren von Microsoft Internet Explorer verwenden, muss der Windows Task-Manager dazu die OpenProcess-Funktion des Microsoft Internet Explorer aufrufen.

Erforderliche Schritte

Die richtige Reaktion auf eine erweiterte Programmwarnung hängt von der Warnungsursache ab. Falls die erweiterte Programmwarnung darauf zurückzuführen ist, dass eine OpenProcess-Funktion aufgerufen wurde, müssen Sie bestimmen, ob die Funktion von einem vertrauenswürdigen oder einem gefährlichen Programm aufgerufen wurde. Stellen Sie sicher, dass das in der Warnung aufgeführte Programm sicher ist und diese Funktion auch ausführen kann. Wenn Sie beispielsweise gerade versucht haben, ein Programm mit dem Windows Task-Manager herunterzufahren, als die erweiterte Programmwarnung angezeigt wurden, ist es mit großer Wahrscheinlichkeit sicher, auf **Ja** zu klicken. Wenn die Warnung durch ein Programm verursacht wurde, das über ein anderes Programm auf das Internet zugreift und dazu regelmäßig eine entsprechende Berechtigung anfordert, ist es ebenfalls mit großer Wahrscheinlichkeit sicher, auf **Ja** zu klicken. Wenn Sie hinsichtlich der Ursache der Warnung oder des erwarteten Verhaltens des Programms, das die Anforderung initiiert hat, unsicher sind, ist es am sichersten, auf **Nein** zu klicken. Nachdem Sie einem Programm eine erweiterte Programmberechtigung verweigert haben, sollten Sie im Internet eine Suche nach dem Dateinamen des Programms durchführen. Sollte es sich um ein gefährliches Programm handeln, finden Sie wahrscheinlich diesbezügliche Informationen und eine Anleitung, wie Sie dieses Programm von Ihrem Computer entfernen können, im Internet.

Reduzieren der Anzahl von erweiterten Programmwarnungen

Normalerweise werden nicht sehr viele erweiterte Programmwarnungen angezeigt. Bei wiederholt auftretenden Warnungen sollten Sie den Programmnamen recherchieren und das Programm ggf. von Ihrem Computer löschen oder dem Programm die notwendigen Zugriffsrechte erteilen.

Warnung „Manuelle Maßnahme erforderlich“

Mit der Warnung Manuelle Maßnahme erforderlich werden Sie darüber informiert, dass weitere Schritte unternommen werden müssen, bevor die Endpoint Security so konfiguriert ist, dass sie Ihre VPN-Verbindung unterstützt.

Bedeutung der Warnung „Manuelle Maßnahme erforderlich“

Die Warnung Manuelle Maßnahme erforderlich tritt auf, wenn die Endpoint Security Ihre VPN-Verbindung nicht automatisch konfigurieren kann oder wenn manuelle Änderungen vorgenommen werden müssen, bevor die Konfiguration abgeschlossen werden kann.

Erforderliche Schritte

Warnungen des Typs "Manuelle Maßnahme erforderlich" erfordern keine Reaktion Ihrerseits. Um die VPN-Verbindung manuell zu konfigurieren, lesen Sie den Abschnitt **Manuelles Konfigurieren der VPN-Verbindung** siehe "[Konfigurieren der VPN-Verbindung](#)" auf Seite 93, und befolgen Sie die Anweisungen zur manuellen Konfiguration.

Reduzieren der Anzahl von Warnungen des Typs „Manuelle Maßnahme erforderlich“

Normalerweise werden nicht sehr viele Warnungen des Typs "Manuelle Maßnahme erforderlich" angezeigt. Falls viele Warnungen angezeigt werden, führen Sie entweder die notwendigen Schritte durch, um die Endpoint Security so zu konfigurieren, dass Ihre VPN-Verbindung unterstützt wird, oder entfernen Sie die VPN-Software von Ihrem Computer.

Warnung Neues Netzwerk

Die Warnung Neues Netzwerk wird angezeigt, wenn Endpoint Security erkennt, dass Sie eine Verbindung zu einem vorher nicht verwendeten Netzwerk hergestellt haben. Über das Warnungsfenster können Sie die Datei- und Druckerfreigabe in diesem Netzwerk aktivieren. Warnungen des Typs "Neues Netzwerk" werden angezeigt, wenn Sie mit einem Netzwerk verbunden sind. Dabei kann es sich um ein Funknetz, ein Unternehmens-LAN oder das Netzwerk Ihres Internetdienstanbieters handeln.

Bei der ersten Verwendung der Endpoint Security wird mit großer Wahrscheinlichkeit die Warnung Neues Netzwerk angezeigt. Diese Warnung ist hilfreich bei der Konfiguration der Endpoint Security.

Bedeutung der Warnung „Neues Netzwerk“

Warnungen des Typs "Neues Netzwerk" werden angezeigt, wenn Sie mit einem Netzwerk verbunden sind. Dabei kann es sich um ein Funknetz, ein Unternehmens-LAN oder das Netzwerk Ihres Internetdienstanbieters handeln.

Standardmäßig wird in Endpoint Security ab Version 3.5 beim Erkennen eines neuen Netzwerks nicht die Warnung Neues Netzwerk, sondern der Netzwerk-Konfigurationsassistent angezeigt.

Erforderliche Schritte

Die Reaktion auf Warnungen des Typs "Neues Netzwerk" hängt von der Netzwerksituation ab.

Falls Sie mit einem Heim- oder lokalen Unternehmensnetzwerk verbunden sind und Ressourcen mit anderen Computern im Netzwerk gemeinsam nutzen möchten, ordnen Sie das Netzwerk der Sicheren Zone zu.

So fügen Sie das neue Netzwerk zur Sicheren Zone hinzu:

1. Geben Sie im Popup-Fenster der Warnung **Neues Netzwerk** in das entsprechende Feld einen Namen für das Netzwerk ein (z. B. Heimnetz).
2. Wählen Sie **Sichere Zone** aus der entsprechenden Dropdown-Liste.
3. Klicken Sie auf OK.

Gehen Sie mit Vorsicht vor, wenn die Endpoint Security ein Funknetzwerk erkennt. Möglicherweise hat Ihre Netzwerkkarte eine Verbindung zu einem anderen als Ihrem eigenen Netzwerk hergestellt. Stellen Sie sicher, dass die in der Warnung "Neues Netzwerk" angezeigte IP-Adresse die IP-Adresse Ihres Netzwerks ist, bevor Sie diese der vertrauenswürdigen Zone hinzufügen.



Wichtig - Wenn Sie nicht sicher sind, welches Netzwerk die Endpoint Security erkannt hat, schreiben Sie die im Warnungsfenster angezeigte IP-Adresse auf. Ziehen Sie die Dokumentation Ihres Heimnetzwerks zu Rate, oder wenden Sie sich an Ihren SystemAdministrator oder Internetdienstanbieter, um herauszufinden, um welches Netzwerk es sich handelt.

Warnung Neues Netzwerk

Es ist ungewöhnlich, viele Warnungen des Typs "Neues Netzwerk" zu erhalten.

Fehlerbehebung

Inhalt dieses Abschnitts

Fehlerbehebung bei VPN	189
Fehlerbehebung für Netzwerke	191
Fehlerbehebung für die Internetverbindung	193

Fehlerbehebung bei VPN

Falls Sie Probleme bei der Verwendung von VPN-Software mit dem Client haben, sehen Sie sich zunächst die Tabelle mit Tipps zur Fehlerbehebung in diesem Abschnitt an.

Table 0-31 Fehlerbehebung bei VPN-Problemen

Falls...	Siehe...
Sie keine Verbindung mit dem virtuellen Privatnetzwerk (VPN) herstellen können	Konfigurieren des Clients für VPN-Datenverkehr auf Seite 190
Erstellen von erweiterten Regeln für Firewallprogramme.	Automatische VPN-Konfiguration und erweiterte Regeln auf Seite 190
Sie einen unterstützten VPN-Client verwenden und Endpoint Security diese Software nicht bei der ersten Erstellung der Verbindung erkennt	Automatische VPN-Erkennungsverzögerung auf Seite 190

Konfigurieren des Clients für VPN-Datenverkehr

Falls Sie keine Verbindung mit Ihrem VPN herstellen können, müssen Sie den Client möglicherweise so konfigurieren, dass von Ihrem VPN eingehender Datenverkehr akzeptiert wird.

So konfigurieren Sie den Client, damit VPN-Datenverkehr zugelassen wird:

1. Fügen Sie VPN-bezogene Netzwerkressourcen zu der Sicherem Zone hinzu.

Siehe **Hinzufügen zur Sicherem Zone** auf Seite [87](#).

2. Richten Sie Zugriffsrechte für den VPN-Client und für alle anderen für das VPN verwendeten Programme auf Ihrem Computer ein.

Siehe **Einstellen spezifischer Berechtigungen** auf Seite [103](#).

3. Lassen Sie VPN-Protokolle zu.

Siehe **Hinzufügen von VPN-Ressourcen zur Sicherem Zone** auf Seite [93](#).

Automatische VPN-Konfiguration und erweiterte Regeln

Falls Sie fortgeschrittene Firewallregeln erstellt haben, die VPN-Protokolle sperren, kann Endpoint Security Client Ihr VPN nicht automatisch erkennen, wenn Sie eine Verbindung initiieren. Um Ihre VPN-Verbindung zu konfigurieren, müssen Sie sicherstellen, dass sich Ihr VPN-Client und die VPN-bezogenen Komponenten in der Sicherem Zone befinden und dass sie über die nötigen Zugriffsrechte für auf das Internet verfügen. Siehe **Manuelles Konfigurieren der VPN-Verbindung** siehe "[Konfigurieren der VPN-Verbindung für Firewall](#)" auf Seite [92](#).

Automatische VPN-Erkennungsverzögerung

Der Endpoint Security Client fragt Ihren Computer in regelmäßigen Abständen ab, ob unterstützte VPN-Protokolle aktiviert sind. Wenn die Protokolle erkannt werden, fordert der Endpoint Security Client Sie auf, Ihre Verbindung automatisch zu konfigurieren. Falls Sie kürzlich einen VPN-Client installiert und versucht haben, eine Verbindung herzustellen, hat der Client Ihre VPN-Konfiguration möglicherweise nicht erkannt. Wenn Sie es vorziehen, dass der Client Ihre Verbindung automatisch konfiguriert, können Sie zehn Minuten warten und dann erneut versuchen, eine Verbindung herzustellen. Versuchen Sie es dann erneut. Falls Sie sofort eine Verbindung herstellen möchten, können Sie Ihre Verbindung manuell konfigurieren. Siehe **Manuelles Konfigurieren der VPN-Verbindung** siehe "[Konfigurieren der VPN-Verbindung für Firewall](#)" auf Seite [92](#).

Fehlerbehebung für Netzwerke

Falls Sie Probleme bei der Aufnahme der Verbindung zu Ihrem Netzwerk oder beim Einsatz der Netzwerkdienste haben, sehen Sie sich die Tabelle mit Fehlerbehebungstipps in diesem Abschnitt an.

Table 0-32 Fehlerbehebung bei Netzwerkproblemen

Falls...	Siehe...
Sie die anderen Computer in der Netzwerkkumgebung nicht sehen können oder diese Computer Ihren Rechner nicht erkennen können	<i>Sichtbarmachen des Computers im lokalen Netzwerk</i> auf Seite 191
Sie keine Dateien und Drucker über Ihr Heimnetzwerk oder lokales Netzwerk freigeben können	<i>Lokales Freigeben von Dateien und Druckern</i> auf Seite 192
Ihr Computer sich in einem lokalen Netzwerk (LAN) befindet und der Systemstart nach Installation von Endpoint Security Client ungewöhnlich lange dauert	<i>Beheben eines langsamen Systemstarts</i> auf Seite 192

Sichtbarmachen des Computers im lokalen Netzwerk

Wenn Sie die anderen Computer in Ihrem lokalen Netzwerk nicht sehen können oder diese Rechner Ihren Computer nicht erkennen, besteht die Möglichkeit, dass der Client den für die Windows-Netzwerksichtbarkeit notwendigen NetBIOS-Datenverkehr sperrt.

So machen Sie Ihren Computer im lokalen Netzwerk sichtbar:

1. Fügen Sie das Subnetz des Netzwerks (oder in kleinen Netzwerken die IP-Adresse aller freigegebenen Computer) der Sicherer Zone hinzu. Siehe ***Hinzufügen zur Sicherer Zone*** auf Seite [87](#).
2. Stellen Sie die Sicherheitsstufe der Sicherer Zone auf **Mittel** und die der Internetzone auf **Hoch**. So wird sicheren Computern Zugriff auf Ihre gemeinsam

genutzten Dateien gewährt, allen anderen Computern jedoch nicht. Siehe **Festlegen von erweiterten Sicherheitsoptionen** auf Seite [81](#).



Hinweis - Der Client erkennt Ihr Netzwerk automatisch und zeigt die Warnung Neues Netzwerk an. Mit der Warnung können Sie das Subnetz des Netzwerks der Sicherer Zone hinzufügen.

Lokales Freigeben von Dateien und Druckern

Mit Endpoint Security Client können Sie Ihren Computer schnell und einfach freigeben, sodass die sicheren Computer, mit denen Sie über ein Netzwerk verbunden sind, auf Ihre freigegebenen Ressourcen zugreifen können. Eindringlinge aus dem Internet jedoch haben keinen Zugriff und können Ihr System nicht gefährden.

So konfigurieren Sie den Client für eine sichere gemeinsame Nutzung von Ressourcen:

1. Fügen Sie das Subnetz des Netzwerks (oder in kleinen Netzwerken die IP-Adresse aller freigegebenen Computer) der Sicherer Zone hinzu. Siehe **Hinzufügen zur Sicherer Zone** auf Seite [87](#).
2. Stellen Sie die Sicherheitsstufe der Sicherer Zone auf **Mittel** ein. Sichere Computer erhalten damit Zugriff auf Ihre freigegebenen Dateien. Siehe **Auswählen der Sicherheitsstufen** auf Seite [80](#).
3. Stellen Sie die Sicherheitsstufe der Internetzone auf **Hoch** ein. Der Computer ist dadurch für nicht in der Sicherer Zone aufgelistete Computer unsichtbar. Siehe **Einstellen der Sicherheitsstufen für Zonen** auf Seite [80](#).

Beheben eines langsamen Systemstarts

Wenn der Client so konfiguriert ist, dass er beim Systemstart geladen wird, kann es vorkommen, dass sich der Startvorgang auf Rechnern in einem lokalen Netzwerk über mehrere Minuten hinzieht.

Dies ist in den meisten Fällen darauf zurückzuführen, dass Ihr Computer Zugriff auf den Domänen-Controller Ihres Netzwerks benötigt, um den Start- und Anmeldevorgang abschließen zu können, und der Client diesen Zugriff sperrt, weil der Controller nicht in die Sichere Zone aufgenommen wurde.

Sie können dieses Problem lösen, indem Sie den Hostnamen oder die IP-Adresse des Domänen-Controllers Ihres Netzwerks zur Sicherer Zone hinzufügen.

Fehlerbehebung für die Internetverbindung

Falls Sie Probleme beim Herstellen einer Verbindung mit dem Internet haben, sehen Sie sich die Tabelle mit Fehlerbehebungstipps in diesem Abschnitt an.

Table 0-33 Beheben von Fehlern bei der Internetverbindung

Falls...	Siehe...
Sie keine Verbindung zum Internet herstellen können	<i>Fehlschlagen der Internetverbindung nach der Installation</i> auf Seite 193
Sie eine Verbindung zum Internet herstellen können, die Verbindung aber nach kurzer Zeit wieder getrennt wird	<i>Zulassen von ISP-Heartbeat-Signalen</i> auf Seite 194
Ihr Computer ein Client der Internetverbindungsfreigabe (ICS) ist und Sie keine Verbindung zum Internet herstellen können	<i>Herstellen einer Verbindung über einen ICS-Client</i> auf Seite 195
Ihr Computer einen Proxyserver verwendet und Sie keine Verbindung zum Internet herstellen können	<i>Herstellen einer Verbindung über einen Proxyserver</i>

Fehlschlagen der Internetverbindung nach der Installation

Wenn Sie nach der Installation von Endpoint Security Client Probleme beim Herstellen einer Internetverbindung haben, sollten Sie zunächst herausfinden, ob die Ursache wirklich bei Endpoint Security Client liegt. Wenn Sie die unten beschriebene Schrittfolge nicht ausführen können (z.B. weil Sie das Kontrollkästchen Endpoint Security beim Systemstart laden nicht deaktivieren können), wenden Sie sich bitte an den technischen Support von Check Point.

So finden Sie heraus, ob die Ursache für die Verbindungsprobleme bei Endpoint Security Client liegt.

1. Öffnen Sie Überblick/Voreinstellungen.
2. Deaktivieren Sie im Bereich Allgemein das Kontrollkästchen Check Point Endpoint Security beim Systemstart laden.

Die Warnung zum Check Point TrueVector-Dienst wird angezeigt.

3. Klicken Sie auf Ja.
4. Starten Sie Ihren Computer neu, und versuchen Sie erneut, eine Verbindung zum Internet herzustellen.

Wenn Sie eine Verbindung herstellen können	liegt der Grund für die Verbindungsprobleme möglicherweise in den Einstellungen von Endpoint Security Client. Vergewissern Sie sich, dass Ihr Browser über Zugriffsrechte verfügt.
Wenn Sie keine Verbindung herstellen können	liegt der Grund für die Verbindungsprobleme nicht in den Einstellungen von Endpoint Security Client.

Zulassen von ISP-Heartbeat-Signalen

Die meisten Internetdienstanbieter senden in regelmäßigen Abständen Heartbeat-Signale an ihre DFÜ-Kunden, um festzustellen, ob der Computer des Kunden noch verbunden ist. Wenn kein angeschlossener Computer erkannt wird, trennt der Internetdienstanbieter unter Umständen die Verbindung und stellt die IP-Adresse einem anderen Benutzer zur Verfügung.

In der Standardeinstellung sperrt Endpoint Security Client die für diese Heartbeat-Signale üblicherweise verwendeten Protokolle. Dies kann dazu führen, dass Ihre Internet-Verbindung getrennt wird. Um dies zu vermeiden, können Sie den Server identifizieren, der die Signale sendet, und diesen Ihrer Sicheren Zone hinzufügen, oder Sie können die Internetzone so konfigurieren, dass Ping-Signale zugelassen werden.

Identifizieren der Quelle der Heartbeat-Signale

Dies ist die bevorzugte Lösung, da sie unabhängig davon funktioniert, ob Ihr Internetdienstanbieter die Verbindung mit NetBIOS oder **ICMP (Internet Control Messaging Protocol)** siehe "ICMP" auf Seite 201 überprüft, und Sie können so die hohe Sicherheitsstufe für die Internetzone beibehalten.

Sie können den Server, von dem aus Ihr Internetdienstanbieter die Verbindung prüft, folgendermaßen erkennen:

1. Klicken Sie nach dem Trennen der Verbindung auf Warnungen & Protokolle | Protokollanzeige.
2. Suchen Sie in der Liste der Warnungen nach der Warnung, die der Uhrzeit entspricht, als Sie die Verbindung getrennt haben.

3. Notieren Sie sich die im Feld **Detailinformationen für Eintrag** angezeigte erkannte Quell-DNS.

Wenn Sie den Server auf diese Weise nicht erkennen können, wenden Sie sich an den Internetdienstanbieter, um herauszufinden, welche Server Zugriffsrechte benötigen.

4. Wenn Sie den Server identifiziert haben, fügen Sie ihn zur Sicherer Zone hinzu.

Siehe **Hinzufügen zur Sicherer Zone** auf Seite [87](#).

Konfigurieren von Endpoint Security Client, um Ping-Signale zuzulassen.

Wenn der Internetdienstanbieter ein ICMP-Echo (oder Ping) zum Überprüfen der Verbindung verwendet, konfigurieren Sie den Client dahingehend, dass Ping-Signale aus der Internetzone zugelassen werden.

So konfigurieren Sie den Client , um Ping-Signale zuzulassen:

1. Öffnen Sie Antivirus/spyware | Grundeinstellungen.
2. Klicken Sie im Internetzonenbereich auf **Benutzerdefiniert**.
3. Aktivieren Sie das Kontrollkästchen **Eingehendes Ping-Signal zulassen (ICMP-Echo)**.
4. Klicken Sie auf **OK**.
5. Setzen Sie die Sicherheitsstufe für die Internetzone auf **Mittel**.

Siehe **Auswählen der Sicherheitsstufen** auf Seite [80](#).

Herstellen einer Verbindung über einen ICS-Client

Wenn Sie die Windows-Option **Gemeinsame Nutzung der Internetverbindung (ICS)** nutzen oder ein Programm eines Drittanbieters zur gemeinsamen Nutzung einer Internetverbindung einsetzen und Sie keine Verbindung zum Internet herstellen können, stellen Sie sicher, dass Endpoint Security Client für die Client- und Gateway-Computer richtig konfiguriert ist. Siehe **Aktivieren der gemeinsamen Nutzung einer Internetverbindung** siehe "[Aktivieren der gemeinsamen Nutzung einer Internetverbindung \("Internet Connection Sharing", ICS\)](#)" auf Seite [80](#).

Konfigurieren Sie den Client nicht für ICS, wenn Sie statt eines Host-PCs Hardware wie beispielsweise einen Server oder Router verwenden.

Herstellen einer Verbindung über einen Proxyserver

Wenn Sie die Verbindung zum Internet über einen Proxyserver erstellen und keine Verbindung herstellen können, stellen Sie sicher, dass sich die IP-Adresse Ihres Proxyservers in der Sicherer Zone befindet. Siehe ***Hinzufügen zur Sicherer Zone*** auf Seite [87](#).

Glossar

Symbols & Numeric

1394

Ein sehr schneller Standard für externe Busse, der Datenübertragungsraten von bis zu 400 Mbit/s (1394a) und 800 Mbit/s (1394b) unterstützt. Die Produkte, die den Standard 1394 unterstützen, haben je nach Unternehmen unterschiedliche Namen. Diese Technologie wurde ursprünglich von Apple entwickelt und trägt bei Apple den markenrechtlich geschützten Namen FireWire.

A

ActiveX-Steuerelemente

ActiveX-Steuerelemente (von Microsoft entwickelt) sind Elemente wie Kontrollkästchen oder Schaltflächen, mit denen Benutzer die Möglichkeit haben, Makros oder Skripts zur Automatisierung einer Aufgabe auszuführen.

Als Server fungieren

Ein Programm fungiert als Server, wenn es auf Verbindungsanfragen anderer Computer reagiert. Einige verbreitete Anwendungen wie Chat-Programme, E-Mail-Programme und Programme zur Internet-Telefonie müssen Serverfunktionen ausführen, um ordnungsgemäß funktionieren zu

können. Allerdings führen auch einige Hackerprogramme Serverfunktionen aus, um Anweisungen ihrer Entwickler entgegennehmen zu können. Der Client hindert alle Programme auf Ihrem Computer in der Internetzone daran, Serverfunktionen auszuführen, es sei denn, Sie weisen diesen Programmen Serverberechtigungen zu.

Animierte Werbung

Eine Werbung, die bewegte Bilder enthält.

B

Bannerwerbung

Eine Werbung, die als waagerechtes Banner über die Breite einer Webseite angezeigt wird.

C

Cache Cleaner

Privatsphärenfunktion, mit der Sie bei Bedarf oder in festgelegten Abständen unerwünschte Dateien und Cookies von Ihrem Computer entfernen können.

Challenge Response

Challenge Response ist ein Authentifizierungsprotokoll, bei dem eine Partei eine Rückfrage stellt und die andere Partei die Antwort liefert. Damit die

Authentifizierung stattfinden kann, muss auf die Frage eine gültige Antwort erfolgen. Sicherheitssysteme, die Smartcards verwenden, basierend auf diesem Authentifizierungsverfahren. Der Benutzer erhält einen Code (die Rückfrage), der in die Smartcard eingegeben wird. Die Smartcard zeigt daraufhin einen neuen Code (die Antwort) an, den der Benutzer für die Anmeldung verwendet.

Cookie

Eine kleine Datendatei, die von einer Website zur Anpassung des Inhalts an den Besucher, zum Erkennen des Besuchers beim nächsten Besuch und zur Verfolgung seiner Internetaktivität verwendet wird. Neben vielen nützlichen Einsatzmöglichkeiten können gewisse Cookies auch dafür verwendet werden, ohne Ihre Zustimmung auf persönliche Informationen zuzugreifen.

Cookie-Einstellungen

Privatsphärenfunktion, mit der Sie verhindern können, dass Cookies auf Ihrem Computer gespeichert werden.

Cookies von Dritten

Ein gespeichertes Cookie, das nicht von der besuchten Website stammt, sondern von einem Werbepartner oder einer anderen Drittpartei. Diese Cookies werden in der Regel dazu eingesetzt, Informationen über Ihre Internetaktivitäten an Dritte weiterzuleiten.

D

DFÜ-Verbindung

Internetverbindung über ein Modem und eine analoge Telefonleitung. Das Modem stellt die Internetverbindung durch telefonische Einwahl beim Internetdienstanbieter her. Damit unterscheidet sich diese Verbindungsart beispielsweise von DSL (Digital Subscriber Lines), bei dem keine Analogmodems verwendet, und keine Telefonnummern angewählt werden.

DHCP

Dynamic Host Configuration Protocol

Ein Protokoll, das die dynamische IP-Adressierung unterstützt. Statt einer statischen IP-Adresse kann Ihnen der Internetdienstanbieter bei jeder Anmeldung eine unterschiedliche IP-Adresse zuweisen. Dadurch reichen dem Internetdienstanbieter relativ wenige IP-Adressen für sehr viele Kunden aus.

DHCP-Rundsendung/Multicast

Ein Nachrichtentyp, der von einem Client-Computer in einem Netzwerk mit dynamischer IP-Adressierung verwendet wird. Beim Herstellen der Verbindung zu einem Netzwerk sendet ein Computer eine Nachricht an einen der DHCP-Server im Netzwerk, wenn er eine IP-Adresse benötigt. Sobald der DHCP-Server die

Nachricht empfängt, weist er dem Computer eine IP-Adresse zu.

DLL

Dynamic Link Library

Eine Bibliothek mit Funktionen, auf die eine Windows-Anwendung dynamisch (d. h. je nach Bedarf) zugreifen kann.

DNS

Domain Name Server

Ein Datenabfragedienst, über den im Internet Hostnamen oder Domännennamen (z.B. www.IhreSeite.de) in eine Internetadresse (z.B. 123.456.789.0) konvertiert werden.

E

Eingebettetes Objekt

Ein Objekt, beispielsweise eine Audio- oder Bilddatei, das in eine Webseite eingebettet ist.

Einstellungen für mobilen Code

Eine Funktion des Clients, die Ihnen die Möglichkeit bietet, aktive Inhalte und Skripts der von Ihnen besuchten Websites zu sperren. Mobiler Code ist im Internet weit verbreitet und hat viele nützliche Einsatzmöglichkeiten, er wird von Hackern jedoch manchmal für schädigende Zwecke verwendet.

Endpoint Security On Demand

Neben einer wirksamen Endpunkt-Konformitätsprüfung (auf erforderliche Softwareupdates,

Anti-Viren-Signaturen usw.) bei der Verbindungsherstellung bietet der Endpoint Security On Demand-Scanner auch die Möglichkeit, Endpunkt-Computer auf potenziell schädliche Software zu untersuchen, bevor der Zugriff auf das interne Netzwerk gewährt wird. Der Zugriff wird Benutzern basierend auf den vom Administrator festgelegten Konformitätsoptionen für das Sicherheits-Gateway gewährt oder verweigert.

Endpoint Security Server

Ein Endpoint Security System von Check Point, das den SystemAdministratoren in die Lage versetzt, die Sicherheit mehrerer Computer von einem einzigen Punkt aus verwalten können. Administratoren erstellen SicherheitsRichtlinien und stellen diese dann für die Endpoint Security Client-Anwendungen auf den Rechnern der Benutzer bereit.

Erstrangige Warnungen

Warnung, der mit hoher Wahrscheinlichkeit ein Hackerangriff zu Grunde liegt. Bei Firewallmeldungen ersten Ranges ist der obere Bereich des Fensters der Warnung rot markiert. In der Protokollanzeige kann eine Warnung ersten Ranges an Hand des Eintrags in der Spalte Klassifizierung erkannt werden.

Erweiterte Einstellungen für Program Control

Die erweiterten Einstellungen für Program Control stellen eine erweiterte Sicherheitsfunktion dar, mit der verhindert wird, dass unbekannte Programme über sichere Programme auf das Internet zugreifen.

G

Gastmodus

Eine Check Point-Lösung für den Remote-VPN-Zugriff, die das Kanalisieren der gesamten Client-/Gateway-Kommunikation über eine gewöhnliche TCP-Verbindung an Port 443 ermöglicht. Der Gastmodus gewährleistet die sichere Kommunikation über Firewalls und ermöglicht das Konfigurieren von Proxyservern zum Sperren von IPSec-Paketen.

Gateway

Eine Kombination aus Hardware und Software, durch die zwei unterschiedliche Netzwerktypen verbunden werden. Wenn Sie z. B. an ein Heim- oder ein Unternehmens-LAN angeschlossen sind, kann über ein Gateway eine Verbindung der Computer in Ihrem Netzwerk mit dem Internet hergestellt werden.

Gespeichertes Cookie

Ein von einer besuchten Website auf Ihrer Festplatte gespeichertes Cookie. Diese Cookies können bei Ihrem nächsten Besuch von der Website abgerufen werden. Obwohl sie nützlich sind, stellen

Cookies durch das Speichern persönlicher Informationen über Sie, Ihren Computer und Ihre Internetnutzung in einer Textdatei eine Schwachstelle dar.

Gespernte Zone

Die Gespernte Zone umfasst alle Computer, mit denen Sie keinen Kontakt wünschen. Der Client unterbindet jeglichen Verkehr zwischen Ihrem Computer und den Computern in dieser Zone.

H

Heartbeat-Signale

Von einem Internetdienstanbieter (ISP) gesendete Signale, mit Hilfe derer der ISP sicher stellt, dass noch eine DFÜ-Verbindung besteht. Wenn kein angeschlossener Computer festgestellt wird, trennt der Internetdienstanbieter unter Umständen die Verbindung und stellt die IP-Adresse einem anderen Benutzer zur Verfügung.

Hinweise

Die Warnungen, die angezeigt werden, wenn der Client eine Datenübertragung sperrt, die gegen Ihre Sicherheitseinstellungen verstößt. Hinweise erfordern keine Reaktion Ihrerseits.

HTTP-Referrer-Header-Feld

Ein optionales Feld in der Meldung, mit dem eine Webseite geöffnet wird. Enthält Informationen über das "verweisende Dokument". Bei

ordnungsgemäßer Verwendung unterstützt dieses Feld den Webmaster bei der Website-Verwaltung. Bei unsachgemäßer Verwendung kann damit Ihre IP-Adresse, der Name Ihres Arbeitsplatzrechners, Ihr Benutzername und (bei schlecht implementierten Websites für E-Commerce) sogar Ihre Kreditkartennummer herausgefunden werden. Indem Sie auf der Registerkarte Cookies die Option Private Überschriftinformationen entfernen auswählen, können Sie verhindern, dass in diesem Überschriftenfeld Informationen über Sie übertragen werden.

I

ICMP

Internet Control Messaging Protocol

Eine Erweiterung des Internetprotokolls (IP), das Fehlersteuerung und Hinweise unterstützt. Ein "Ping" ist ein übliches ICMP-Signal zum Testen von Internetverbindungen.

ICS

Gemeinsame Nutzung der Internetverbindung

ICS ist ein Windows-Dienst, mit dem eine einzelne Internetverbindung in einem Netzwerk gemeinsam genutzt werden kann.

IKE

Internet Key Exchange (Internet-Schlüsselaustausch) ist ein vom IPSec-Protokoll für folgende Zwecke verwendetes Verfahren:

- Authentifizieren von Benutzern
- Verhandeln des Verschlüsselungsverfahrens
- Austausch eines geheimen Schlüssels für die Datenverschlüsselung

Index.dat

Index.dat-Dateien speichern Cookies zu allen Informationen in Ihren temporären Internet-, Cookies- und Verlaufsordnern, sogar NACHDEM diese Dateien gelöscht wurden.

Integriertes MIME-Type-Objekt

Ein Objekt, beispielsweise eine Bild-, Audio- oder Videodatei, das in eine E-Mail integriert ist. MIME steht für "Multipurpose Internet Mail Extensions".

Internetzone

Die Internetzone umfasst alle Computer weltweit, mit Ausnahme der Computer, die Sie der Sicheren Zone oder der Gesperrten Zone zugeordnet haben.

Der Client wendet die höchsten Sicherheitsanforderungen im Umgang mit der Internetzone an und schützt Sie so vor Hackern. Die mittleren Sicherheitseinstellungen für die Sichere Zone erlauben es Ihnen unterdessen, problemlos Daten

mit Computern oder Netzwerken auszutauschen, denen Sie vertrauen (z.B. Computer in Ihrem Heim- oder Unternehmensnetzwerk).

IP-Adresse

An Hand dieser Nummer wird Ihr Computer im Internet identifiziert. Dies ist mit einer Telefonnummer vergleichbar, durch die Ihr Telefon in einem Telefonnetz identifiziert wird. Die IP-Adresse ist eine numerische Adresse, meist vier durch Punkte getrennte Zahlen zwischen 0 und 255. Ein Beispiel einer IP-Adresse wäre 172.16.100.100.

Ihre IP-Adresse kann immer die gleiche sein. Es kann auch sein, dass Ihr Internetdienstanbieter (ISP, Internet Service Provider) das Dynamic Host Configuration Protocol (DHCP) einsetzt und Ihrem Computer bei jeder Einwahl in das Internet eine andere IP-Adresse zugewiesen wird.

IPSec

Ein Sicherheitsprotokoll für die Authentifizierung und Verschlüsselung über das Internet.

ISP

Internet Service Provider

Ein Unternehmen, das Zugriff auf das Internet anbietet. ISPs bieten Privat- und Geschäftskunden eine Vielzahl unterschiedlicher Internetzugänge, z. B. DFÜ-Verbindungen (Verbindung über eine normale Telefonleitung mittels Modem),

Hochgeschwindigkeits-DSL und Kabelmodem.

J

Java-Applet

Ein Java-Applet ist ein kleines Internet-basiertes Programm, das in Java geschrieben wurde und normalerweise in einer HTML-Seite auf einer Website eingebettet ist und im Browser ausgeführt werden kann.

JavaScript

Eine verbreitete Skriptsprache, welche die Grundlage einiger der häufigsten interaktiven Inhalte auf Websites bildet. Zu diesen häufig genutzten JavaScript-Funktionen gehören unter anderem Links, die eine oder mehrere Seiten zurückblättern, beim Darüberfahren mit der Maus wechselnd angezeigte Grafiken sowie das Öffnen und Schließen von Browserfenstern. Die Standardeinstellungen lassen JavaScript zu, weil es so geläufig und meistens harmlos ist.

K

Key Fobs

Ein *Key Fob* ist ein kleines Hardwaregerät mit einem integrierten Authentifizierungsmechanismus zum Steuern des Zugriffs auf Netzwerkdienste und Informationen. Während ein Kennwort ohne Wissen des Eigentümers gestohlen werden kann, wird ein fehlendes Key Fob sofort bemerkt. Key Fobs bieten

ebenso wie andere SecurID-Geräte eine zweistufige Authentifizierung: Der Benutzer besitzt eine PIN (Personal Identification Number), die ihn als Besitzer des Gerätes ausweist. Nachdem der Benutzer seine PIN eingegeben hat, zeigt das Gerät eine Nummer an, mit der die Anmeldung beim Netzwerk erfolgt. Das Key Fob SecurID SID700 ist ein gutes Beispiel für ein solches Gerät.

Komponente

Ein kleines Programm oder eine Auswahl an Funktionen, auf die über größere Programme zum Durchführen bestimmter Aufgaben zugegriffen werden kann. Einige Komponenten können von verschiedenen Programmen gleichzeitig verwendet werden. Unter Windows stehen viele Komponenten als DLL (Dynamic Link Library/Programmbibliothek) für verschiedene Windows-Anwendungen zur Verfügung.

L

Lernmodus für Komponenten

Der Zeitraum nach der Installation, wenn die Programmeinstellung auf **Mittel** eingestellt ist. Im Lernmodus für Komponenten erlernt der Client schnell die MD5-Signaturen häufig verwendeter Komponenten, ohne dass Ihre Arbeit durch zahlreiche Warnungen unterbrochen wird.

M

Mailserver

Der Remote-Computer, über den Ihr Computer die an Sie gesendeten E-Mails abruft.

MD5-Signatur

Digitaler "Fingerabdruck", an Hand dessen die Echtheit und Integrität von Daten geprüft werden kann. Wenn ein Programm in irgendeiner Form verändert wurde (z.B. bei der Manipulation durch einen Hacker), dann ändert sich auch die MD5-Signatur.

Mobiler Code

Ausführbarer Inhalt, der in eine Webseite oder HTML-E-Mail eingebettet werden kann. Mit mobilem Code werden Websites interaktiv gestaltet, gefährlicher mobiler Code kann jedoch für Datenänderungen, -diebstahl oder sonstige schädigende Zwecke verwendet werden.

N

NetBIOS

Network Basic Input/Output System

Ein Programm, mit dem Anwendungen auf unterschiedlichen Computern Daten über ein lokales Netzwerk austauschen können. Der Client lässt standardmäßig NetBIOS-Datenverkehr in der Sicheren Zone zu, sperrt diesen jedoch in der Internetzone. Dadurch ist die gemeinsame Nutzung von Dateien in lokalen Netzwerken möglich,

während zugleich der Schutz vor NetBIOS-Angriffen aus dem Internet gewährleistet ist.

O

Öffentliches Netzwerk

Ein großes Netzwerk, wie beispielsweise das eines Internetdienstanbieters. Öffentliche Netzwerke werden standardmäßig der Internetzone zugeordnet.

P

Paket

Eine einzelne Dateneinheit im Netzwerkverkehr. In "paketvermittelten" Netzwerken wie dem Internet wird ausgehender Datenverkehr in kleine Einheiten aufgeteilt, an den Empfänger gesendet und dort wieder zusammengesetzt. Jedes Paket enthält die IP-Adresse des Absenders und die IP-Adresse und Port-Nummer des Empfängers.

Persönliche Richtlinie

Ihre persönliche Richtlinie umfasst alle Sicherheitseinstellungen, die Sie über die Oberfläche des Clients steuern können. Wenn Sie zum Beispiel über die Registerkarte Zonen einen Server zur Sicheren Zone hinzufügen, wird diese Konfiguration Bestandteil Ihrer persönlichen Richtlinie.

Ping

Eine ICMP-Nachricht (auch "ICMP-Echo" genannt), mit der festgestellt werden kann, ob ein

Computer mit dem Internet verbunden ist. Ein kleines Dienstprogramm sendet eine "Echoanforderung" an die IP-Adresse des Empfängers und wartet dann auf eine Antwort. Wenn ein Computer unter der angegebenen Adresse die Nachricht erhält, sendet er ein "Echo" zurück. Einige Internetdienstanbieter senden regelmäßig Ping-Signale aus, um festzustellen, ob ihre Kunden noch mit dem Internet verbunden sind.

Popunder-Werbung

Eine Werbung in einem neuen Browserfenster, das hinter dem derzeit angezeigten Fenster eingeblendet wird. Sie sehen die Werbung also erst, wenn Sie das ursprüngliche Browserfenster schließen.

Popup-Werbung

Eine Werbung in einem neuen Browserfenster, das vor dem derzeit angezeigten Fenster eingeblendet wird.

Port

Ein mit der Verwendung von TCP oder UDP verknüpfter Kanal. Einige Ports werden standardmäßig von bestimmten Netzwerkprotokollen belegt. Für HTTP (Hypertext Transfer Protocol) wird z.B. üblicherweise Port80 verwendet. Die Portnummern liegen im Bereich von 0 bis 65535.

Portscan

Eine Hackertechnik, mit der ungeschützte Computer im Internet aufgespürt werden können. Der Hacker verwendet dabei ein Programm, das automatisch und systematisch alle Ports auf den Computern eines IP-Bereichs überprüft und ungesicherte oder "offene" Ports entdeckt. Über einen offenen Port kann ein Hacker Zugriff auf einen ungeschützten Computer erhalten.

Private Überschrift

Ein Webseiten-Abschnitt, in dem Informationen zur Website enthalten sind und Informationen über Besucher der Website gesammelt werden können. Durch private Überschriftinformationen können Websites, auf die Sie durch einen Link auf einer anderen Website gekommen sind, herausfinden, von welcher Website aus Sie auf diese Website gelangt sind. Falls eine Website private Überschriften nicht vorsichtig einsetzt, können über diese privaten Überschriften Informationen, die Sie in einem Webformular eingegeben haben (z. B. Ihre Kreditkartennummer oder Sozialversicherungsnummer) übertragen werden.

Privater Speicher

Ein Zertifikatscontainer auf Ihrem Computer (im Gegensatz zu einem Zertifikat für ein Token). Er steht erst zur Verfügung, nachdem Sie auf das Betriebssystem zugreifen können.

Programmliste

Liste mit Programmen, denen Sie Zugriffsrechte für das Internet und Serverberechtigungen zuweisen können. Die Liste wird im Fenster **Program Control** auf der Registerkarte **Programme** angezeigt. Sie können Programme zur Liste hinzufügen oder daraus entfernen.

Protokoll

Standardformat zum Senden und Empfangen von Daten. Die einzelnen Protokolle dienen verschiedenen Aufgaben; so wird z.B. SMTP (Simple Mail Transfer Protocol) beim Versand von E-Mails verwendet, FTP (File Transfer Protocol) hingegen bei der Übertragung großer Dateien verschiedener Formate. Jedes Protokoll ist einem bestimmten Port zugeordnet. FTP-Sendungen werden z.B. an Port21 adressiert.

Q

Quarantäne

MailSafe stellt eingehende E-Mail-Anhänge unter Quarantäne, wenn deren Dateinamenerweiterung (z. B. EXE oder BAT) darauf hinweist, dass unter Umständen selbsttätig ausführbarer Code enthalten ist. Durch Ändern der Dateinamenerweiterung wird verhindert, dass unter Quarantäne gestellte Anhänge ohne Überprüfung geöffnet werden. Dies schützt Sie vor Würmern, Viren und anderer gefährlicher Software, die von Hackern in Form

von E-Mail-Anhängen verbreitet werden.

R

Ratgeber zur Privatsphäre

Eine kleine Anzeige, die Sie darüber informiert, wenn der Client Cookies oder mobilen Code sperrt, und Ihnen die Möglichkeit bietet, diese Elemente für eine bestimmte Seite zu entsperren.

Remote Access Community

Remote Access Community ist ein Typ einer VPN-Gemeinschaft speziell für Benutzer, die normalerweise an entfernten Standorten außerhalb des Unternehmens-LAN arbeiten.

Remote-Zugriff auf VPN

Bezieht sich auf Remote-Benutzer, die mit Client-Software, z. B. Endpoint Connect, auf das Netzwerk zugreifen. Das Connectra-Gateway bietet Remote-Zugriff für Remote-Clients.

S

SecurID

Der RSA SecurID-Authentifizierungsmechanismus besteht aus Hardware (FOB, USB-Token) oder Software (SoftID), die in festen Intervallen (normalerweise eine Minute) anhand einer integrierten Uhr und eines zufälligen, codierten Schlüssels einen Authentifizierungscode generiert.

Die häufigste Form des SecurID-Tokens ist das Handgerät. Das

Gerät ist normalerweise ein Key Fob oder eine Slimcard. Das Token kann über eine PIN-Tastatur verfügen, über die der Benutzer eine PIN (Personal Identification Number) eingibt, um einen **Passcode** zu generieren. Besitzt das Token *keine* PIN-Tastatur, wird ein **Tokencode** angezeigt. Der **Tokencode** ist die wechselnde Zahl, die auf dem Key Fob angezeigt wird.

Serverberechtigung

Mit der Serverberechtigung kann ein Programm auf Ihrem Computer die Verbindungsanfrage eines anderen Computers empfangen und schließlich eine Verbindung aufbauen. Im Unterschied dazu wird einem Programm durch Zugriffsrechte gestattet, eine Verbindungsanfrage an einen anderen Computer zu senden. Einige gängige Anwendungen wie Chat-Programme, E-Mail-Programme und Programme mit Internet-Anklopf Funktion benötigen Serverberechtigungen, damit sie ordnungsgemäß funktionieren. Erteilen Sie Serverberechtigungen nur wirklich sicheren Programmen, die diese Rechte für ein ordnungsgemäßes Funktionieren benötigen. Erteilen Sie möglichst keine Serverberechtigungen für die Internetzone. Wenn Sie eingehende Verbindungen von nur wenigen Computern akzeptieren müssen, fügen Sie diese Computer einfach Ihrer Sicheren Zone hinzu, und gewähren Sie dem Programm

nur für die Sichere Zone
Serverberechtigungen.

Sichere Zone

Die Sichere Zone umfasst alle Computer, mit denen Sie ohne Bedenken Ressourcen austauschen können.

Wenn Sie z.B. drei PCs in einem Ethernet-Heimnetzwerk haben, können Sie entweder jeden einzelnen Computer oder das gesamte Netzwerkadapter-Subnetz der Sicheren Zone zuordnen. Mit der voreingestellten mittleren Sicherheitsstufe der Sicheren Zone können Sie Dateien, Drucker und andere Ressourcen in Ihrem Heimnetzwerk freigeben. Hacker werden auf die Internetzone beschränkt. Dort sorgen die hohen Sicherheitseinstellungen für Ihren Schutz.

Sicherheitsstufen

Die Einstellungen **Hoch**, **Mittel** und **Niedrig**, die die Art des zulässigen eingehenden und ausgehenden Datenverkehrs definieren.

Sitzungs-Cookie

Ein im Cache-Speicher des Browsers gespeichertes Cookie, das beim Schließen des Browserfensters gelöscht wird. Dank ihrer kurzen Lebensdauer sind dies die sichersten Cookies.

Skript

Eine Reihe von Befehlen, die automatisch ausgeführt werden, ohne dass der Benutzer eingreift. In der Regel in Form von Bannern,

Popup-Werbung oder Menüs, die sich ändern, wenn der Mauszeiger darüber bewegt wird.

SmartDefense Advisor

Der SmartDefense Advisor von Check Point ist ein Online-Dienstprogramm, mit dem Sie eine Warnung sofort auf ihre mögliche Ursache hin untersuchen können. Dies ist hilfreich bei der Entscheidung, ob auf eine Warnung des Programms mit Ja oder mit Nein geantwortet werden soll. Klicken Sie im Fenster der Warnung auf die Schaltfläche **Mehr Info**, um den SmartDefense Advisor aufzurufen. Der Client leitet daraufhin Informationen zur Warnung an den SmartDefense Advisor weiter. Sie erhalten vom SmartDefense Advisor einen Artikel, in dem die Warnung erklärt wird und Sie ggf. darüber informiert werden, was zu tun ist, um Ihre Sicherheit weiterhin zu gewährleisten.

SoftID

SoftID funktioniert genau wie ein Passcode-Gerät, besteht jedoch ausschließlich aus Software, die auf dem PC installiert ist.

In der erweiterten Ansicht werden Tokencode und Passcode mit Kopieren-Schaltflächen angezeigt, mit denen der Benutzer Daten zwischen SoftID und Client kopieren und einfügen kann.

Stealth-Modus

Wenn der Client Ihren Computer in den Stealth-Modus versetzt,

bleibt jeder unaufgeforderte Datenverkehr unbeantwortet. So lässt sich von außen nicht einmal erkennen, dass Ihr Computer existiert. Ihr Computer bleibt für andere Computer im Internet unsichtbar, bis ein berechtigtes Programm auf Ihrem Computer eine Verbindung herstellt.

T

TCP

TCP (Transmission Control Protocol)

Eines der Hauptprotokolle in TCP/IP-Netzwerken, das die Übertragung von Daten garantiert und sicherstellt, dass Pakete in der gleichen Reihenfolge ankommen, in der sie abgesendet wurden.

Trojaner

Ein gefährliches Programm, das sich als harmlose oder nützliche Anwendung tarnt (z.B. als Bildschirmschoner). Einige Trojaner können sich als Server auf Ihrem Computer installieren und Verbindungen von außen überwachen. Gelingt es einem Hacker, eine Verbindung mit dem Programm herzustellen, kann er Ihren Computer kontrollieren. Deshalb sollten Sie Serverberechtigungen nur Programmen gewähren, die Sie kennen und denen Sie vertrauen. Andere Trojaner versuchen, automatisch eine Verbindung zu einer externen Adresse herzustellen.

TrueVector-Sicherheitsengine

Die wichtigste Sicherheitskomponente der Client-Sicherheit. Die TrueVector-Engine untersucht den Internet-Datenverkehr und erzwingt Sicherheitsregeln.

U

UDP

UDP (User Datagram Protocol)

Ein Protokoll ohne Verbindung, dass über IP-Netzwerken ausgeführt wird und hauptsächlich zum Senden von Nachrichten über ein Protokoll verwendet wird.

UnternehmensRichtlinie

Eine Gruppe von Sicherheitseinstellungen (Firewall, Program Control, E-Mail-Schutz usw.), die von einem NetzwerkAdministrator erstellt, und dem Client durch Laden vom Endpoint Security Server übergeben wird. Der Endpunktbenutzer kann die UnternehmensRichtlinie nicht ändern.

V

Vertikales Werbebanner

Eine Werbung, die als Säule seitlich auf einer Webseite angezeigt wird.

VPN

Virtual Private Network

Ein VPN ist ein Netzwerk, das sicheren, privaten Zugriff auf ein LAN (z. B. das Netzwerk Ihres Unternehmens) über öffentliche

Infrastrukturen (wie das Internet) bereitstellt. Dabei werden die Übertragungen und Daten über Verschlüsselungsprotokolle und andere Sicherheitsmaßnahmen getunnelt.

W

Web Bug

Eine Bilddatei, häufig 1×1Pixel groß, die für die Überwachung der Aufrufe der Seite (oder HTML-E-Mail) eingesetzt wird, in der sie enthalten ist. Web Bugs werden oft eingesetzt, um zu ermitteln, welche Werbung und welche Webseiten Sie angezeigt haben.

Werbeblocker

Eine Funktion des Clients, die Ihnen die Möglichkeit bietet, Banner, Popup-Fenster und andere Typen von Werbung zu sperren.

Z

Zugriffsberechtigung

Mit Zugriffsrechten kann ein Programm auf Ihrem Computer eine Kommunikationsverbindung zu einem anderen Computer herstellen. Der Unterschied zu Serverberechtigungen besteht darin, dass mit diesen einem Programm gestattet wird, Verbindungsanfragen von einem anderen Computer entgegenzunehmen. Sie können einem Programm Zugriffsrechte für die Sichere Zone, die Internetzone oder für beide Zonen gewähren.

Zweitrangige Warnung

Eine Warnung, die wahrscheinlich durch harmlose Netzwerkaktivitäten und nicht durch einen Hackerangriff ausgelöst wurde.

Index

1

1394 - 197

A

ActiveX-Steuerelemente - 197

Aktivieren der automatischen Sperre -
100, 177

Aktivieren der automatischen Spyware-
Behandlung - 70

Aktivieren der automatischen
Virenbehandlung - 69

Aktivieren der Datei- und Druckerfreigabe
- 79

Aktivieren der gemeinsamen Nutzung
einer Internetverbindung (- 80, 195

Aktivieren der Protokollierung - 45

Aktivieren des Hub Mode (Hub-Modus) -
50

Aktivieren des Office Mode (Büromodus) -
49

Aktualisieren von Antivirus und Anti-
Spyware - 58

Aktualisieren von Sites - 39

Aktualisieren von Viren- und Spyware-
Definitionen - 66

Als Server fungieren - 197

Ändern der Anmeldeinformationen für die
Authentifizierung - 128

Ändern der Sprache für die
Benutzeroberfläche - 129

Ändern des Kennworts für das
verschlüsselte Gerät - 146

Ändern von Authentifizierungsverfahren -
24, 39

Ändern von Profilen - 34

Ändern von Zonen-Datenverkehrsquellen -
86

Angaben von Spyware-
Erkennungsmethoden - 69

Animierte Werbung - 197

Anmelden bei aktivierter SSO- oder
OneCheck Logon-Funktion - 125

Anpassen der Einstellungen von Program
Control - 102

Anpassen der Ereignisprotokollierung -
167

Anpassen der Programmprotokollierung -
168

Anpassen des MailSafe-Schutzes für
ausgehenden Datenverkehr - 156

Anti-Spyware Ausnahmeliste - 73

Antivirus / Anti-Spyware - 13

Antivirus und Anti-Spyware - 57

Antivirus und Anti-Spyware aktivieren - 57

Antivirus-Ausnahmenliste - 72

Anzeigen der verfügbaren Richtlinien -
160

Anzeigen des Textprotokolls - 170

Anzeigen des Viren- und Spyware-
Schutzstatus - 58

Anzeigen von Elementen in Quarantäne -
62

Anzeigen von Profileigenschaften - 35

Anzeigen von Protokolleinträgen - 168

Anzeigen von Protokollen - 63
Anzeigen von Site-Eigenschaften - 39
Anzeigen von Status- und
Verschlüsselungsinformationen - 126
Anzeigen von Zonendatenverkehr - 86
Archivieren von Protokolleinträgen - 171
Aufheben der Auswahl der SSO-Option -
124
Ausschließen einer
Computermanipulierung - 116
Auswählen der Sicherheitsstufen - 80,
192, 195
Ausweichsprachen - 131
Authentifizierung - 24
Authentifizierung bei Full Disk Encryption
- 115
Auto Local Logon (Autom. lokale
Anmeldung) - 23, 47
Auto-Connect (Autom. Verbindung) - 46
Automatische VPN-
Erkennungsverzögerung - 189, 190
Automatische VPN-Konfiguration und
erweiterte Regeln - 189, 190
Autorisieren von Wechselmedien - 146

B

Bannerwerbung - 197
Bedeutung der Programmwarnungen - 185
Bedeutung der Warnung - 179, 180, 182,
183, 186, 187
Bedeutung von Einhaltungswarnungen -
177
Bedeutung von Meldungen für
Internetsperre - 176
Bedeutung von Warnungen bei gesperrtem
Programm - 176

Befehlszeilenoptionen - 54
Behandeln von Elementen in Quarantäne -
63
Beheben eines langsamen Systemstarts -
191, 192
Bereich - 148
Bildschirm - 14
Bildschirme - 13

C

Cache Cleaner - 197
Challenge Response - 197
Cookie - 198
Cookie-Einstellungen - 198
Cookies von Dritten - 198

D

Das Auftreten von Firewallmeldungen
verringern. - 174
Deaktivieren des Schutzes für ausgehende
E-Mails - 107
Deaktivieren von Popup-Meldungen - 53
Deaktivieren von Sites - 40
Definieren von Sites - 37
DFÜ-Support - 52
DFÜ-Verbindung - 198
DHCP - 198
DHCP-Rundsendung/Multicast - 198
DLL - 98, 199
DNS - 199

E

Ein- und Ausblenden von Firewall-
Warnungen - 166

Ein- und Ausblenden von Warnungen - 166

Einführung in Endpoint Security - 11

Eingebettetes Objekt - 199

Einhaltungswarnungen - 19, 177

Einstellen der Authentifizierungsoptionen - 108

Einstellen der Zugriffsrechte für Programme - 101

Einstellen grundlegender Warn- und Protokolloptionen - 165

Einstellen spezifischer Berechtigungen - 103, 113, 156, 190

Einstellung für hohe Sicherheit - 77

Einstellung für mittlere Sicherheit - 77

Einstellungen für mobilen Code - 199

Einstellungen für Standard-Portberechtigungen - 89, 111

E-Mail-Schutz - 14, 155

Encryption Richtlinie Manager - 136

Endpoint Security Antivirus und Anti-Spyware - 57

Endpoint Security On Demand - 199

Endpoint Security Server - 199

Erforderliche Schritte - 174, 175, 176, 177, 179, 180, 181, 182, 184, 186, 187, 188

Erneuern von Check Point-Zertifikaten - 30

Erste Anmeldung nach Aktivierung von SSO oder OneCheck Logon - 124

Erstellen einer Desktop-Verknüpfung für ein Profil - 35

Erstellen einer PKCS#12-Datei für ein Check Point-Zertifikat - 27

Erstellen eines CAPI-Token für ein Check Point-Zertifikat - 28

Erstellen von Profilen - 32

Erstmalige Authentifizierung - 116

Erstrangige Warnungen - 199

Erteilen der Berechtigung zum Senden von E-Mails für Programme - 106

Erteilen der Serverberechtigung für Programme - 106, 110, 112, 184, 185

Erweiterte Einstellungen für Program Control - 106, 200

Erweiterte Konfigurationsoptionen - 53

Erweiterte Optionen - 65

Erweiterte Programmwarnungen - 185

Exportieren und Importieren von Profilen - 33

Extrahieren von Dateien auf die lokale Festplatte - 145

Extrahieren von Dateien in einen sicheren temporären Speicherort - 145

F

Fehlerbehebung - 189

Fehlerbehebung bei VPN - 189

Fehlerbehebung für die Internetverbindung - 193

Fehlerbehebung für Netzwerke - 191

Fehlschlagen der Internetverbindung nach der Installation - 193

Festlegen allgemeiner Sicherheitsoptionen - 83

Festlegen der Ereignis- und Programmprotokollierungsoptionen - 165, 167

Festlegen der Optionen von Program Control - 98

Festlegen der Sicherheitsstufe für Program Control - 99

Festlegen der Warnungsereignisstufe - 165

Festlegen des Kennworts auf Benutzerebene - 15

Festlegen von allgemeinen Voreinstellungen - 16

Festlegen von erweiterten Sicherheitsoptionen - 81, 112, 192

Festlegen von Gateway-Sicherheitsoptionen - 81

Festlegen von ICS-Optionen - 82

Festlegen von Netzwerk-Sicherheitsoptionen - 85

Festlegen von Verbindungsvoreinstellungen - 17

Festlegen von Voreinstellungen - 15

Festlegen von Zielen für die Prüfung - 67

Firewall - 13, 75

Firewallmeldung/Geschützt - 173

Firewall-Schutz verstehen - 75

Format der Protokollarchivierung - 167

Freigeben des VPN-Gateway - 94

Führung durch das Endpoint Security-Hauptseite - 11

Full Disk Encryption - 14, 115

Full Disk Encryption-Statusinformationen - 126

Funktionen - 135

G

Gastmodus - 200

Gateway - 81, 200

Gelber Meldebanner - 151

Gerätemanager - 136, 137

Gespeichertes Cookie - 200

Gespernte Zone - 76, 200

Gewähren von Internet-Zugriffsrechten für Programme - 105, 110, 184

Gewähren von Zugriffsrechten für VPN-Software - 95

Gründe für das Auftreten von Firewallmeldungen - 174

Gründe für das Auftreten von MailSafemeldungen - 175

Grundlegendes zu Program Control - 97

Grundlegendes zu Prüfungsergebnissen - 60

Grundlegendes zu Verbindungsdetails - Rechts-VPN - 42

Grundlegendes zu Verbindungseinstellungen - Endpoint Connect VPN - 45

Grundlegendes zu Verbindungsinformationen - Endpoint Connect VPN - 44

Grundlegendes zu Warnungen und Protokollen - 163

Grundlegendes zu WebCheck - 149

Grundlegendes zu Zonen - 76

Grundlegendes zur Registerkarte - 17

Grundlegendes zur Vermittlung zwischen Richtlinie - 160

H

Heartbeat-Signale - 200

Herstellen einer Verbindung über einen Hotspot. - 49

Herstellen einer Verbindung über einen ICS-Client - 193, 195

Herstellen einer Verbindung über einen Proxyserver - 196

Herstellen einer Verbindung zu Netzwerk-Mailservern - 79

Herstellen und Trennen von Verbindungen - 41

Hinweise - 164, 173, 200

Hinzufügen benutzerdefinierter Ports - 91

Hinzufügen von Programmen zur Programmliste - 104, 181

Hinzufügen von VPN-Ressourcen zur Sicherer Zone - 93, 190

Hinzufügen zur Gesperrten Zone - 89

Hinzufügen zur Sicherer Zone - 78, 79, 87, 109, 112, 113, 114, 190, 191, 192, 195, 196

HTTP-Referrer-Header-Feld - 200

I

ICMP - 194, 201

ICS - 82, 201

Identifizieren der Quelle der Heartbeat-Signale - 194

IKE - 201

In der Vorstart-Umgebung unterstützte Zeichen - 134

Index.dat - 201

Informationen zu Warnungen - 163

Informationen zur Ereignisprotokollierung - 164

Informationen zur Full Disk Encryption-Lizenzaktivierung - 127

Integrieren in Netzwerkdienste - 78

Integrierte Windows-Anmeldung - 125

Integriertes MIME-Type-Objekt - 201

Internet-Modus - 150

Internet-Modus und Unternehmensmodus - 150

Internetzone - 76, 201

IP-Adresse - 202

IPSec - 202

ISP - 202

J

Java-Applet - 202

JavaScript - 202

K

Kein Zugriff auf den Token/die Smartcard - 121

Key Fobs - 202

Klonen von Profilen - 34

Kompakte und erweiterte VPN-Oberflächen - 22, 32

Komponente - 203

Konfigurieren der VPN-Verbindung - 93, 187

Konfigurieren der VPN-Verbindung für Firewall - 92, 190

Konfigurieren des Clients für VPN-Datenverkehr - 189, 190

Konfigurieren des Programmzugriffs - 101

Konfigurieren neuer Netzwerkverbindungen - 78

Konfigurieren von Endpoint Security Client, um Ping-Signale zuzulassen. - 195

Konfigurieren von Profilen und Sites - 31

Konfigurieren von Verbindungsoptionen - 46

L

Lernmodus für Komponenten - 203
Lokales Freigeben von Dateien und
Druckern - 191, 192
Löschen von CDs oder DVDs - 146
Löschen von Profilen - 36
Löschen von Sites - 23, 40

M

MailSafe nach Programm aktivieren - 156
MailSafemeldung - 175
Mailserver - 203
Manager für Wechselmedien - 136
Manuelle Behandlung von Dateien - 60
MD5-Signatur - 203
Media Encryption - 14, 135
Meldungen für Internetsperre - 176
Mobiler Code - 203

N

NAT Traversal Tunneling - 39, 53
Navigieren durch das Endpoint Security-
Hauptseite - 12
NetBIOS - 80, 203

O

Öffentliches Netzwerk - 204
Optionale Full Disk Encryption-Funktionen
- 121
Optionen für die Virenprüfung - 71

P

Paket - 204
Persönliche Richtlinie - 204
Ping - 204

Planen von Prüfungen - 65
Popunder-Werbung - 204
Popup-Werbung - 204
Port - 204
Portscan - 205
Private Überschrift - 205
Privater Speicher - 205
Program Control - 13, 97
Program Control über Zonen - 77
Program Security Guard - 137
Programmauthentifizierung - 98, 182
Programmliste - 205
Programmwarnungen - 164, 178
Protokoll - 205
Protokollanzeigefelder - 169
Proxy-Einstellungen (Visitor Mode
(Gastmodus)) - 51
Prüfen - 59
Prüfen bei Zugriff - 68

Q

Quarantäne - 205

R

Ratgeber zur Privatsphäre - 206
Reagieren auf Warnungen - 18
Reduzieren der Anzahl von
Einhaltungswarnungen - 178
Reduzieren der Anzahl von erweiterten
Programmwarnungen - 186
Reduzieren der Anzahl von Meldungen für
Internetsperre - 177
Reduzieren der Anzahl von Warnungen bei
gesperrtem Programm - 176

Reduzieren der Anzahl von Warnungen des
Typs - 179, 180, 181, 183, 185, 187

Remote Access Community - 206

Remote-Zugriff auf VPN - 206

Reparieren von Dateien in einem Archiv -
70

Richtlinie Typen - 159

Richtlinien - 14, 65, 159

Rote Warnmeldungen - 153

Rote Warnung - 152

S

Schutz durch WebCheck - 149

Schutz für ausgehenden MailSafeverkehr -
155, 156, 157, 175

Secure Domain Logon (Sichere
Anmeldung über Domäne) - 23, 47

SecurID - 206

Senden von Viren und Spyware an Check
Point - 61

Serverberechtigung - 77, 206

Sichere Zone - 76, 207

Sicherheitsstufen - 80, 207

Sichtbarmachen des Computers im
lokalen Netzwerk - 191

Single Sign-On und OneCheck Logon -
123

Sitzungs-Cookie - 207

Skript - 207

SmartDefense Advisor - 207

SoftID - 207

Speichern des Zertifikats an einem
anderen Speicherort - 29

Speichern von PKCS#12-Dateien im
CAPI-Speicher - 29

Sperren und Freigeben von Ports - 77, 89

SSO, OneCheck Logon und
Kennwortänderungen - 124

Starten und Beenden von VPN-Client-
Diensten - 23

Stealth-Modus - 207

Synchronisieren von Kennwörtern - 122

T

Taskleisten-Symbole - 12

TCP - 208

Trojaner - 208

TrueVector-Sicherheitsengine - 208

Typen von Endpoint Security VPNs - 22

U

UDP - 208

Unternehmensmodus - 151

UnternehmensRichtlinie - 208

Unterstützte Sprachen - 130

Unterstützte VPN-Protokolle - 92

V

Verbindung immer herstellen - 48

Verbindungsstatus - 42

Verschlüsseln von CDs und DVDs - 142

Verschlüsseln von Medien - 139, 142

Verschlüsselungsinformationen - 128

Vertikales Werbebanner - 208

Verwalten von Check Point Zertifikaten -
27

Verwalten von Entrust-Zertifikaten - 26

Verwalten von Programmkomponenten -
108

Verwalten von Verbindungsprofilen - 32
Verwalten von VPN-Sites - 36
Verwalten von Zertifikaten - 25, 37
Verwalten von Zonendatenverkehr - 85
Verwaltung der Firewall-Sicherheit nach Zonen - 76
Verwenden der Fernsteuerung - 112
Verwenden der Programmliste - 103
Verwenden der Registerkarte - 15, 58
Verwenden des Bildschirms Richtlinien - 160
Verwenden des EPM Clients - 139
Verwenden des Full Disk Encryption-Bildschirms - 126
Verwenden des Full Disk Encryption-Kennworts für Windows - 123
Verwenden des Gerätemanagers - 147
Verwenden des Managers für Wechselmedien - 146
Verwenden des Windows-Kennworts für Full Disk Encryption - 122
Verwenden einer Smartcard/eines USB-Tokens - 119
Verwenden eines dynamischen Tokens - 118
Verwenden eines festen Kennworts - 116
Verwenden von Antivirus-Software - 109
Verwenden von Browsern - 109
Verwenden von Chat-Programmen - 110
Verwenden von E-Mail - 110
Verwenden von Filesharing - 111
Verwenden von FTP - 111
Verwenden von internetbasierten Anrufbeantworterdiensten - 111

Verwenden von Program Security Guard - 148
Verwenden von Programmen mit dem Client - 109
Verwenden von SmartDefense Advisor - 172, 185
Verwenden von Spielen - 112
Verwenden von Streaming Media - 112
Verwenden von VNC - 113
Verwenden von Voice over IP (VoIP) - 113
Verwenden von Web Conferencing - 114
Vorgehensweise bei einem vergessenen Kennwort - 121
VPN - 13, 21, 208
VPN – Grundlagen - 21
VPN-Protokolle zulassen - 94

W

Warnung - 18, 19, 178, 179, 180, 181, 183, 186
Warnung Neues Netzwerk - 164, 187, 188
Warnungen bei gesperrtem Programm - 175
Warnungen und Protokolle - 163
Warnungen vor verdächtigen Sites - 151
Warnungsmeldungen - Referenz - 163, 173
Web Bug - 209
WebCheck - 14, 149
Wechseln zwischen den Modi - 151
Werbeblocker - 209

Z

Zugreifen auf verschlüsselte Medien - 142

Zugreifen auf verschlüsselte Medien von
Computern ohne Media Encryption -
144

Zugriffsberechtigung - 77, 209

Zugriffssteuerung für Programme - 97

Zulassen der Verwendung von
Programmen durch andere Benutzer -
108

Zulassen von ISP-Heartbeat-Signalen -
175, 193, 194

Zweitrangige Warnung - 209

Zwischengespeicherte Kennwörter - 138